Guide de l'utilisateur

AWS CloudTrail

Version 1.0

AWS CloudTrail: Guide de l’utilisateur

Table of Contents

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

AWS CloudTrail est un outil Service AWS qui vous aide à permettre l'audit des opérations et des risques, la gouvernance et la conformité de votre Compte AWS. Les actions entreprises par un utilisateur, un rôle ou un AWS service sont enregistrées sous forme d'événements dans CloudTrail. Les événements incluent les actions entreprises dans le AWS Management Console, AWS Command Line Interface, ainsi que dans AWS les SDK et les API.

CloudTrail est actif dans votre Compte AWS lorsque vous le créez. Lorsqu'une activité se produit dans votre environnement Compte AWS, cette activité est enregistrée dans un CloudTrail événement.

CloudTrail propose trois méthodes pour enregistrer des événements :

- Historique des événements : l'Historique des événements fournit un enregistrement consultable, interrogeable, téléchargeable et immuable des événements de gestion des 90 derniers jours dans une Région AWS. Vous pouvez effectuer des recherches d'événement en filtrant sur un seul attribut. Vous avez automatiquement accès à l'Historique des événements lorsque vous créez votre compte. Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.

  La consultation de CloudTrail l'historique des événements est gratuite.
- CloudTrail Lake — AWS CloudTrail Lake est un lac de données géré permettant de capturer, de stocker, d'accéder et d'analyser l'activité des utilisateurs et des API à AWS des fins d'audit et de sécurité. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement, qui sont des ensembles inaltérables d'événements basés sur des critères que vous sélectionnez en appliquant les sélecteurs d'événements avancés. Vous pouvez conserver les données d'événement dans une banque de données d'événement jusqu'à 3 653 jours (environ 10 ans) si vous choisissez l'option de tarification de rétention extensible d'un an, ou jusqu'à 2 557 jours (environ 7 ans) si vous choisissez l'option de tarification de rétention de sept ans. Vous pouvez créer un magasin de données d'événements pour un Compte AWS ou plusieurs événements Comptes AWS en utilisant AWS Organizations. Vous pouvez importer tous les CloudTrail journaux existants de vos compartiments S3 dans un magasin de données d'événements existant ou nouveau. Vous pouvez également visualiser les principales tendances en matière CloudTrail d'événements avec les tableaux de bord Lake. Pour plus d'informations, consultez Travailler avec AWS CloudTrail Lake.

CloudTrail Les stockages et requêtes de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Lorsque vous exécutez des requêtes dans Lake, vous payez en fonction de la quantité de données analysées. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

- Trails : les sentiers enregistrent les AWS activités, diffusent et stockent ces événements dans un compartiment Amazon S3, avec une livraison optionnelle à CloudWatch Logs et Amazon EventBridge. Vous pouvez saisir ces événements dans vos solutions de surveillance de la sécurité. Vous pouvez également utiliser vos propres solutions tierces ou des solutions telles qu'Amazon Athena pour rechercher et analyser vos CloudTrail journaux. Vous pouvez créer des parcours pour un Compte AWS ou plusieurs Comptes AWS en utilisant AWS Organizations. Vous pouvez journaliser les événements Insights pour analyser vos événements de gestion afin de détecter tout comportement anormal en termes de volumes d'appels d'API et de taux d'erreur. Pour plus d'informations, consultez Création d'un parcours pour votre Compte AWS.

  Vous pouvez envoyer gratuitement une copie de vos événements de gestion en cours à votre compartiment S3 CloudTrail en créant une trace. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

La visibilité de l'activité de votre AWS compte est un aspect essentiel de la sécurité et des meilleures pratiques opérationnelles. Vous pouvez l'utiliser CloudTrail pour afficher, rechercher, télécharger, archiver, analyser et répondre à l'activité des comptes dans l'ensemble de votre AWS infrastructure. Vous pouvez identifier qui ou quoi a pris telle ou telle mesure, quelles ressources ont été utilisées, quand l'événement s'est produit, ainsi que d'autres informations pour vous aider à analyser l'activité de votre AWS compte et à y répondre.

Vous pouvez CloudTrail intégrer des applications à l'aide de l'API, automatiser la création de magasins de données de suivi ou d'événements pour votre organisation, vérifier l'état des magasins de données d'événements et des journaux que vous créez, et contrôler la façon dont les utilisateurs visualisent les CloudTrail événements.

Accès CloudTrail

Vous pouvez travailler avec CloudTrail l'une des méthodes suivantes.

Rubriques

- CloudTrail console
- AWS CLI
- CloudTrail API
- AWS SDK

CloudTrail console

Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.

La CloudTrail console fournit une interface utilisateur permettant d'effectuer de nombreuses CloudTrail tâches telles que :

- Consulter les événements récents et l'historique des événements de votre AWS compte.
- Téléchargement d'un fichier filtré ou complet des événements de gestion des 90 derniers jours à partir de l'historique des événements.
- Création et modification de CloudTrail pistes.
- Création et modification de magasins de données d'événements CloudTrail Lake.
- Exécution de requêtes sur des stockages de données d'événement.
- Configuration des CloudTrail sentiers, notamment :
  - Sélection d'un compartiment Amazon S3 pour journaux de suivi.
  - Définition d'un préfixe.
  - Configuration de la livraison vers CloudWatch Logs.
  - Utilisation de AWS KMS clés pour le chiffrement des données de suivi.
  - Activation des notifications Amazon SNS pour la transmission de fichiers journaux sur les journaux de suivi.
  - Ajout et gestion des identifications pour vos journaux de suivi.
- Configuration des magasins de données d'événements CloudTrail Lake, notamment :

- Intégrer des magasins de données d'événements avec des CloudTrail partenaires ou avec vos propres applications, afin de consigner des événements provenant de sources extérieures AWS.
- Fédérer des banques de données d'événements pour exécuter des requêtes depuis Amazon Athena.
- Utilisation de AWS KMS clés pour le chiffrement des données du magasin de données relatives aux événements.
- Ajout et gestion des balises pour vos magasins de données d'événement.

Pour plus d'informations sur le AWS Management Console, consultez AWS Management Console.

AWS CLI

AWS Command Line Interface Il s'agit d'un outil unifié avec lequel vous pouvez interagir à CloudTrail partir de la ligne de commande. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Command Line Interface. Pour une liste complète des commandes CloudTrail CLI, consultez cloudtrail et cloudtrail-data dans la référence des commandes.AWS CLI

CloudTrail API

Outre la console et la CLI, vous pouvez également utiliser les API CloudTrail RESTful pour programmer CloudTrail directement. Pour plus d'informations, consultez la référence AWS CloudTrail d'API et la référence d'API CloudTrail -Data.

AWS SDK

Au lieu d'utiliser l' CloudTrail API, vous pouvez utiliser l'un des AWS SDK. Chaque Kit de développement logiciel (SDK) se compose de bibliothèques et d'exemples de code pour différents langages et plateformes de programmation. Les SDK constituent un moyen pratique de créer un accès programmatique à. CloudTrail Par exemple, vous pouvez utiliser des Kits de développement logiciel (SDK) pour signer de façon chiffrée des demandes, gérer les erreurs et lancer de nouvelles tentatives de demande automatiquement. Pour plus d'informations, consultez la AWS page Outils pour créer.

Comment CloudTrail fonctionne

Vous avez automatiquement accès à l'historique des CloudTrail événements lorsque vous créez votre Compte AWS. L'Historique des événements fournit un enregistrement consultable,

interrogeable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés d'une Région AWS.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrail Lake.

Rubriques

CloudTrail Historique de l'événement

Vous pouvez facilement consulter les événements de gestion des 90 derniers jours dans la CloudTrail console en accédant à la page Historique des événements. Vous pouvez également consulter l'historique des événements en exécutant la commande aws cloudtrail lookup-events ou l'opération d'API `LookupEvents`. Vous pouvez effectuer des recherches d'événement dans Event history (Historique des événements) en filtrant les événements via un seul attribut. Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.

L'Historique des événements n'est pas connecté aux journaux de suivi ou aux entrepôts de données d'événement présents dans votre compte et n'est pas affecté par les modifications de configuration que vous apportez à vos journaux de suivi et entrepôts de données d'événement.

L'affichage de la CloudTrail page d'historique des événements ou l'exécution de la `lookup-events` commande sont gratuits.

CloudTrail Magasins de données sur les lacs et les événements

Vous pouvez créer un magasin de données d'événements pour enregistrer les CloudTrail événements (événements de gestion, événements de données), les événements CloudTrail Insights, les AWS Audit Manager preuves, les éléments de AWS Config configuration ou les événements extérieurs à AWS.

Les magasins de données d'événements peuvent enregistrer des événements provenant du compte actuel Région AWS ou de tous Régions AWS les événements de votre AWS compte. Les magasins

de données d'événements que vous utilisez pour enregistrer des événements d'intégration provenant de l'extérieur AWS doivent être destinés à une seule région ; ils ne peuvent pas être des magasins de données d'événements multirégionaux.

Si vous avez créé une organisation dans AWS Organizations, vous pouvez créer un magasin de données d'événements d'organisation qui enregistre tous les événements pour tous les AWS comptes de cette organisation. Les magasins de données d'événement d'organisation peuvent s'appliquer à l'ensemble des régions AWS ou à la région actuelle. Les entrepôts de données d'événement d'organisation doivent être créés à l'aide du compte de gestion ou du compte de l'administrateur délégué et, lorsqu'il est spécifié qu'ils s'appliquent à une organisation, ils sont automatiquement appliqués à tous les comptes membres de l'organisation. Les comptes membres ne peuvent pas afficher le magasin de données d'événement d'organisation, ni le modifier ou le supprimer. Les banques de données d'événements de l'organisation ne peuvent pas être utilisées pour collecter des événements provenant de l'extérieur de AWS. Pour plus d'informations, consultez Magasins de données d'événement d'organisation.

Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés par CloudTrail. Lorsque vous configurez un magasin de données d'événements, vous pouvez choisir d'utiliser le vôtre AWS KMS key. L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée. Pour plus d'informations, consultez Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS).

Le tableau suivant fournit des informations sur les tâches que vous pouvez effectuer sur les banques de données d'événements.

Tâche	Description
Afficher les tableaux de bord de Lake	Vous pouvez utiliser les tableaux de bord CloudTrail Lake pour visualiser les événements dans les magasins de données d'événements qui collectent des événements de gestion, des événements de données S3 ou des événements Insights.
Événements de gestion des journaux	Configurez votre banque de données d'événements pour consigner les événements en lecture seule, en écriture seule ou tous les événements de gestion. Par défaut, les données relatives aux événements stockent les événements de gestion des journaux.

Tâche	Description
Enregistrer les événements liés aux données	Configurez votre banque de données d'événements pour enregistrer les événements de données. Vous pouvez utiliser des sélecteurs d'événements avancés pour filtrer les `eventName` `readOnly`, et des `resources.ARN` champs pour enregistrer uniquement les événements qui vous intéresse nt.
Événements Log Insights	Configurez vos entrepôts de données d'événement pour journaliser les événements Insights afin de vous aider à identifier les activités inhabituelles associées aux appels d'API de gestion et à y répondre. Pour plus d'informations, consultez Journalisation des événements Insights. Des frais supplémentaires s'appliquent pour les événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.
Copier les événements du trail	Vous pouvez copier les événements du parcours dans un magasin de données d'événements nouveau ou existant pour créer un point-in-time instantané des événements enregistrés dans le parcours.
Activer la fédération sur un magasin de données d'événements	Vous pouvez fédérer un magasin de données d'événements pour voir les métadonnées associées au magasin de données d'événements dans le catalogue de AWS Glue données et exécuter des requêtes SQL sur les données d'événements à l'aide d'Amazon Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger.

Tâche	Description
Arrêter ou démarrer l'ingestion d'événements dans un magasin de données d'événements	Vous pouvez arrêter et démarrer l'ingestion d'événements dans les magasins de données d'événements qui collectent CloudTrail des événements de gestion et de données, ou des éléments AWS Config de configuration.
Créez une intégration avec une source d'événements en dehors de AWS	Vous pouvez utiliser les intégrations CloudTrail Lake pour enregistrer et stocker les données d'activité des utilisateurs provenant de l'extérieur AWS, de n'importe quelle source dans vos environnements hybrides, telles que des applications internes ou SaaS hébergées sur site ou dans le cloud, des machines virtuelles ou des conteneurs. Pour plus d'informations sur les partenaires d'intégration disponibles, consultez AWS CloudTrail Lake Integrations.
Afficher des exemples de requêtes Lake dans la CloudTrail console	La CloudTrail console fournit un certain nombre d'exemples de requêtes qui peuvent vous aider à commencer à écrire vos propres requêtes.
Création ou modification d'une requête	Les requêtes in CloudTrail sont créées en SQL. Vous pouvez créer une requête dans l'onglet CloudTrail Lake Editor en écrivant la requête en SQL à partir de zéro, ou en ouvrant une requête enregistrée ou un exemple de requête et en la modifiant .
Enregistrer les résultats de la requête dans un compartiment S3	Lorsque vous exécutez une requête, vous pouvez enregistrer les résultats de la requête dans un compartiment S3.
Télécharger les résultats de requête enregistrés	Vous pouvez télécharger un fichier CSV contenant les résultats de vos requêtes CloudTrail Lake enregistrés.
Valider les résultats de requête enregistrés	Vous pouvez utiliser CloudTrail la validation de l'intégrité des résultats de requête pour déterminer si les résultats de la requête ont été modifiés, supprimés ou inchangés après CloudTrail leur transmission au compartiment S3.

Pour plus d'informations sur CloudTrail Lake, consultezTravailler avec AWS CloudTrail Lake.

CloudTrail Les stockages et requêtes de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Lorsque vous exécutez des requêtes dans Lake, vous payez en fonction de la quantité de données analysées. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

CloudTrail sentiers

Un journal de suivi est une configuration qui permet la transmission d'événements à un compartiment Amazon S3 que vous spécifiez. Vous pouvez également diffuser et analyser des événements dans un journal avec Amazon CloudWatch Logs et Amazon EventBridge.

Les sentiers peuvent enregistrer les événements CloudTrail de gestion, les événements liés aux données et les événements Insights.

Vous pouvez créer deux types de sentiers pour un Compte AWS : les sentiers multirégionaux et les sentiers à région unique.

Sentiers multirégionaux

Lorsque vous créez un journal multirégional, enregistrez CloudTrail les événements dans l'ensemble Régions AWS de la AWS partition sur laquelle vous travaillez et délivre les fichiers journaux d' CloudTrail événements dans un compartiment S3 que vous spécifiez. Si un Région AWS est ajouté après avoir créé un parcours multirégional, cette nouvelle région est automatiquement incluse et les événements de cette région sont enregistrés. La création d'un journal de suivi multi-régions est une bonne pratique recommandée, car vous pouvez journaliser l'activité dans toutes les régions dans votre compte. Tous les sentiers que vous créez à l'aide de la CloudTrail console sont multirégionaux. Vous pouvez convertir un parcours à région unique en un parcours multirégional à l'aide du. AWS CLI Pour plus d'informations, consultez Créer un journal de suivi dans la console et Convertir un journal de suivi qui s'applique à une région de sorte qu'il s'applique à toutes les régions.

Sentiers d'une seule région

Lorsque vous créez un parcours d'une seule région, CloudTrail enregistre les événements de cette région uniquement. Il fournit ensuite les fichiers journaux d' CloudTrail événements à un

compartiment Amazon S3 que vous spécifiez. Vous ne pouvez créer un journal de suivi à région unique qu'à l'aide de l' AWS CLI. Si vous créez des pistes uniques supplémentaires, vous pouvez faire en sorte que ces pistes fournissent des fichiers journaux d' CloudTrail événements dans le même compartiment S3 ou dans des compartiments séparés. Il s'agit de l'option par défaut lorsque vous créez un parcours à l'aide de l'API AWS CLI ou de l' CloudTrail API. Pour plus d'informations, consultez Création, mise à jour et gestion de sentiers à l'aide du AWS CLI.

> **Note**
>
> Pour les deux types de journaux de suivi, vous pouvez spécifier un compartiment Amazon S3 de n'importe quelle région.

Si vous avez créé une organisation dans AWS Organizations, vous pouvez créer un journal d'organisation qui enregistre tous les événements pour tous les AWS comptes de cette organisation. Les parcours d'organisation peuvent s'appliquer à toutes les AWS régions ou à la région actuelle. Les journaux de suivi d'une organisation doivent être créés en utilisant le compte de gestion et, s'il est spécifié qu'ils s'appliquent à une organisation, ils sont automatiquement appliqués à tous les comptes membres de l'organisation. Les comptes membres peuvent consulter l'historique de l'organisation, mais ne peuvent ni le modifier ni le supprimer. Par défaut, les comptes membres n'ont pas accès aux fichiers journaux d'un journal de suivi d'organisation dans le compartiment Amazon S3.

Par défaut, lorsque vous créez un journal dans la CloudTrail console, vos fichiers journaux d'événements sont chiffrés à l'aide d'une clé KMS. Si vous choisissez de ne pas activer le chiffrement SSE-KMS, vos journaux d'événements sont chiffrés à l'aide du chiffrement côté serveur (SSE) Amazon S3. Vous pouvez stocker vos fichiers journaux dans votre compartiment aussi longtemps que vous le souhaitez. Vous pouvez également définir des règles de cycle de vie d'Amazon S3 pour archiver ou supprimer les fichiers journaux automatiquement. Si vous souhaitez recevoir des notifications lors de la transmission et de la validation des fichiers journaux, vous pouvez configurer des notifications Amazon SNS.

CloudTrail publie des fichiers journaux plusieurs fois par heure, environ toutes les 5 minutes. Ces fichiers journaux contiennent les appels d'API provenant des services du compte qui les prennent en charge CloudTrail. Pour plus d'informations, consultez CloudTrail services et intégrations pris en charge.

> **Note**
>
> CloudTrail fournit généralement des journaux dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti. Pour plus d'informations, consultez le Contrat de niveau de service (SLA)AWS CloudTrail.
> Si vous configurez mal votre trace (par exemple, si le compartiment S3 est inaccessible), vous CloudTrail tenterez de remettre les fichiers journaux à votre compartiment S3 pendant 30 jours, et ces attempted-to-deliver événements seront soumis aux frais standard. CloudTrail Pour éviter des frais sur un journal de suivi mal configuré, vous devez supprimer le journal de suivi.
> CloudTrail capture les actions effectuées directement par l'utilisateur ou pour le compte de l'utilisateur par un AWS service. Par exemple, un AWS CloudFormation `CreateStack` appel peut entraîner des appels d'API supplémentaires vers Amazon EC2, Amazon RDS, Amazon EBS ou d'autres services tels que requis par le modèle. AWS CloudFormation Ce comportement est normal et attendu. Vous pouvez déterminer si l'action a été entreprise par un AWS service grâce au `invokedby` champ figurant dans l' CloudTrailévénement.

Le tableau suivant fournit des informations sur les tâches que vous pouvez effectuer sur les sentiers.

Tâche	Description
Événements de gestion de la journalisation	Configurez vos parcours pour enregistrer les événements en lecture seule, en écriture seule ou tous les événements de gestion.
Enregistrer les événements liés aux données	Vous pouvez utiliser des sélecteurs d'événements avancés pour créer des sélecteurs précis afin de n'enregistrer que les événements de données qui vous intéressent. Lorsque vous utilisez des sélecteurs d'événements avancés, vous pouvez filtrer le `eventName` champ pour inclure ou exclure la journalisation d'appels d'API spécifiques, ce qui permet de contrôler les coûts.

Tâche	Description
Événements Log Insights	Configurez vos journaux de suivi pour journaliser les événements Insights afin de vous aider à identifier les activités inhabituelles associées aux appels d'API de gestion et à y répondre. Des frais supplémentaires s'appliquent pour les événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.
Afficher les événements Insights	Après avoir activé CloudTrail Insights on a trail, vous pouvez consulter jusqu'à 90 jours d'événements Insights à l'aide de la CloudTrail console ou du AWS CLI.
Télécharger les événements Insights	Après avoir activé CloudTrail Insights on a trail, vous pouvez télécharger un fichier CSV ou JSON contenant les événements Insights des 90 derniers jours pour votre trail.
Copiez les événements du sentier sur CloudTrail le lac	Vous pouvez copier les événements de randonnée existants dans un magasin de données d'événements CloudTrail Lake pour créer un point-in-time instantané des événements enregistrés sur le sentier.

Tâche	Description
Créer une rubrique Amazon SNS et s'y abonner	Abonnez-vous à une rubrique pour recevoir des notifications concernant la livraison de fichiers journaux dans votre compartiment. Amazon SNS peut vous avertir de diverses manières, y compris par programmation à l'aide d'Amazon Simple Queue Service. **Note** Si vous souhaitez recevoir des notifications SNS relatives aux livraisons de fichiers journaux de toutes les régions, spécifiez une seule rubrique SNS pour votre journal de suivi. Si vous souhaitez traiter tous les événements par programmation, consultez Utilisation de la bibliothèque CloudTrail de traitement.
Afficher vos fichiers journaux	Recherchez et téléchargez vos fichiers journaux depuis le compartiment S3.

Tâche	Description
Surveillez les événements avec CloudWatch les journaux	Vous pouvez configurer votre journal pour envoyer des événements à CloudWatch Logs. Vous pouvez ensuite utiliser CloudWatch les journaux pour surveiller votre compte afin de détecter des appels et des événements d'API spécifiques. **Note** Si vous configurez un suivi qui s'applique à toutes les régions pour envoyer des événements à un groupe de CloudWatch journaux, CloudTrail envoie les événements de toutes les régions à un seul groupe de journaux.
Activer le chiffrement des journaux	Le chiffrement des fichiers journaux offre une couche de sécurité supplémentaire pour vos fichiers journaux.
Activer l'intégrité des fichiers journaux	La validation de l'intégrité des fichiers journaux vous permet de vérifier que les fichiers journaux sont restés inchangés depuis leur CloudTrail livraison.
Partagez des fichiers journaux avec d'autres Comptes AWS	Vous pouvez partager des fichiers journaux entre les comptes.
Agréger les journaux de plusieurs comptes	Vous pouvez agréger les fichiers journaux provenant de plusieurs comptes dans un seul compartiment.

Tâche	Description
Travaillez avec des solutions partenaires	Analysez vos CloudTrail résultats à l'aide d'une solution partenaire qui s'intègre à CloudTrai l. Les solutions partenaires offrent une large gamme de fonctionnalités, telles que le journal de suivi des modifications, la résolution de problèmes et l'analyse de sécurité.

Vous pouvez envoyer une copie de vos événements de gestion en cours à votre compartiment S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Événements Insights

AWS CloudTrail Insights aide AWS les utilisateurs à identifier les activités inhabituelles associées aux appels d'API et aux taux d'erreur des API et à y répondre en analysant en permanence les événements CloudTrail de gestion. CloudTrail Insights analyse vos modèles habituels de volume d'appels d'API et de taux d'erreur d'API, également appelés référence, et génère des événements Insights lorsque le volume d'appels ou les taux d'erreur sont en dehors des modèles normaux. Les événements Insights sur le volume d'appels d'API sont générés pour les API de gestion `write`, et les événements Insights sur le taux d'erreur de l'API sont générés pour les API de gestion `read` et `write`.

Par défaut, les magasins de données de CloudTrail parcours et d'événements n'enregistrent pas les événements Insights. Vous devez configurer votre banque de données de parcours ou d'événements pour consigner les événements Insights. Pour plus d'informations, consultez Enregistrement des événements Insights à l'aide du AWS Management Console et Enregistrement des événements Insights à l'aide du AWS Command Line Interface.

Des frais supplémentaires s'appliquent pour les événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.

Affichage des événements Insights pour les sentiers et les magasins de données sur les événements

CloudTrail prend en charge les événements Insights à la fois pour les sentiers et les magasins de données d'événements, mais il existe certaines différences dans la façon dont vous visualisez et accédez aux événements Insights.

Affichage des événements Insights pour les journaux de suivi

Si les événements Insights sont activés sur un parcours et que vous CloudTrail détectez une activité inhabituelle, les événements Insights sont enregistrés dans un dossier ou un préfixe différent du compartiment S3 de destination de votre parcours. Vous pouvez également voir le type d'aperçu et la période de l'incident lorsque vous consultez les événements Insights sur la CloudTrail console. Pour plus d'informations, consultez Afficher CloudTrail les événements Insights relatifs aux parcours dans la CloudTrail console.

Une fois que vous avez activé CloudTrail Insights pour la première fois sur un trail, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 36 heures, si une activité inhabituelle est détectée.

Affichage des événements Insights pour les entrepôts de données d'événement

Pour enregistrer les événements Insights dans CloudTrail Lake, vous avez besoin d'un magasin de données d'événements de destination qui enregistre les événements Insights et d'un magasin de données d'événements source qui active Insights et enregistre les événements de gestion. Pour plus d'informations, consultez Créez un magasin de données d'événements pour les événements CloudTrail Insights à l'aide de la console.

Une fois que vous avez activé CloudTrail Insights pour la première fois dans le magasin de données d'événements source, la transmission du premier événement Insights CloudTrail au magasin de données d'événements de destination peut prendre jusqu'à 7 jours, si une activité inhabituelle est détectée.

Si CloudTrail Insights est activé sur un magasin de données d'événements source et que vous CloudTrail détectez une activité inhabituelle, CloudTrail transmet les événements Insights à votre magasin de données d'événements de destination. Vous pouvez ensuite interroger votre banque de données d'événements de destination pour obtenir des informations sur vos événements Insights et éventuellement enregistrer les résultats de la requête dans un compartiment S3. Pour plus d'informations, consultez Créer ou modifier une requête et Afficher des exemples de requêtes dans la CloudTrail console.

Vous pouvez consulter le tableau de bord Insights Events pour visualiser les événements Insights dans votre banque de données d'événements de destination. Pour de plus amples informations sur le tableau de bord Lake, veuillez consulter Afficher les tableaux de bord de CloudTrail Lake.

CloudTrail chaînes

CloudTrail prend en charge deux types de canaux :

Canaux pour les intégrations de CloudTrail Lake avec des sources d'événements extérieures à AWS

CloudTrail Lake utilise des canaux pour transmettre des événements provenant de AWS l'extérieur à CloudTrail Lake par des partenaires externes qui travaillent avec CloudTrail ou depuis vos propres sources. Lorsque vous créez un canal, vous sélectionnez un ou plusieurs magasins de données d'événement pour stocker les événements provenant de la source du canal. Vous pouvez modifier les stockages de données d'événement de destination d'un canal selon vos besoins, à condition qu'ils soient configurés pour journaliser les événements d'activité. Lorsque vous créez un canal pour les événements d'un partenaire externe, vous fournissez un ARN de canal au partenaire ou à l'application source. La politique de ressources attachée au canal permet à la source de transmettre des événements via celui-ci. Pour plus d'informations, veuillez consulter les sections Créez une intégration avec une source d'événements en dehors de AWS et `CreateChannel` (français non garanti) de la Référence d'API AWS CloudTrail .

Canaux liés à un service

AWS les services peuvent créer un canal lié au service pour recevoir des CloudTrail événements en votre nom. Le AWS service qui crée le canal lié au service configure les sélecteurs d'événements avancés pour le canal et indique si le canal s'applique à toutes les régions ou à la région actuelle.

Vous pouvez utiliser la CloudTrail console ou AWS CLIpour afficher des informations sur les canaux CloudTrail liés à un service créés par. Services AWS

CloudTrail concepts

Cette section résume les concepts de base liés à. CloudTrail

Concepts :

- CloudTrail événements

- Historique des événements
- Journaux de suivi
- Sentiers d'organisation
- CloudTrail Magasins de données sur les lacs et les événements
- CloudTrail Perspectives
- Balises
- AWS Security Token Service et CloudTrail
- Événements de services mondiaux

CloudTrail événements

Un événement dans CloudTrail est l'enregistrement d'une activité sur un AWS compte. Cette activité peut être une action entreprise par une identité IAM ou un service contrôlable par. CloudTrail CloudTrailles événements fournissent un historique de l'activité des comptes API et non-API effectuée via les AWS SDK AWS Management Console, les outils de ligne de commande et d'autres AWS services.

CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

CloudTrail enregistre trois types d'événements :

- Événements de gestion
- Événements de données
- Événements Insights

Tous les types d'événements utilisent un format de journal CloudTrail JSON.

Par défaut, les journaux de suivi et les entrepôts de données d'événement consignent les événements de gestion, mais pas les événements de données ou les événements Insights.

Pour plus d'informations sur le mode Services AWS d'intégration avec CloudTrail, consultezAWS sujets de service pour CloudTrail.

Événements de gestion

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom opérations de plan de contrôle.

Les événements de gestion sont notamment les suivants :

- Configuration de la sécurité (par exemple, les opérations d' AWS Identity and Access Management `AttachRolePolicy`API).
- Enregistrement des appareils (par exemple, les opérations d'API `CreateDefaultVpc` Amazon EC2).
- Configuration des règles de routage des données (par exemple, les opérations d'API `CreateSubnet` Amazon EC2).
- Configuration de la journalisation (par exemple, les opérations d' AWS CloudTrail `CreateTrail`API).

Les événements de gestion peuvent aussi inclure les événements non API qui se produisent dans votre compte. Par exemple, lorsqu'un utilisateur se connecte à votre compte, CloudTrail enregistre l'`ConsoleLogin`événement. Pour plus d'informations, consultez Événements non liés à l'API capturés par CloudTrail.

Par défaut, les données relatives aux événements relatifs aux CloudTrail sentiers et aux CloudTrail lacs stockent les événements de gestion des journaux. Pour plus d'informations sur la journalisation des événements de gestion, consultezJournalisation des événements de gestion.

Événements de données

Les événements de données fournissent des informations sur les opérations de ressource exécutées sur ou dans une ressource. Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé.

Les événements de données incluent notamment :

- Activité de l'API au niveau des objets Amazon S3 (par exemple, `GetObject``DeleteObject`, et opérations d'`PutObject`API) sur des objets dans des compartiments S3.
- AWS Lambda activité d'exécution de fonctions (l'`Invoke`API).

- CloudTrail `PutAuditEvents`activité sur un chenal CloudTrail lacustre utilisé pour enregistrer des événements provenant de l'extérieur AWS.
- Opérations d'API `Publish` et `PublishBatch` d'Amazon SNS sur des rubriques.

Le tableau suivant indique les types d'événements de données disponibles pour les journaux de suivi et les entrepôts de données d'événement. La colonne Type d'événement de données (console) indique la sélection appropriée dans la console. La colonne de valeur resources.type indique la `resources.type` valeur que vous devez spécifier pour inclure les événements de données de ce type dans votre magasin de données de suivi ou d'événement à l' AWS CLI aide des API or. CloudTrail

Pour les traces, vous pouvez utiliser des sélecteurs d'événements de base ou avancés pour enregistrer les événements de données relatifs aux objets Amazon S3, aux fonctions Lambda et aux tables DynamoDB (illustrés dans les trois premières lignes du tableau). Vous ne pouvez utiliser que des sélecteurs d'événements avancés pour enregistrer les types d'événements de données indiqués dans les lignes restantes.

Pour les entrepôts de données d'événement, vous ne pouvez utiliser que des sélecteurs d'événements avancés pour inclure les événements de données.

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon DynamoDB	Activité de l'API au niveau des éléments Amazon DynamoDB sur les tables (par exemple`PutItem`,`Delem`, et les opérations d'API). `UpdateItem` **Note** Pour les tables ayant	DynamoDB	`AWS::DynamoDB::Table`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	les flux activés, le champ `resources` dans l'événement de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les		

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	événement s de flux, ajoutez un filtre sur le `eventName` champ.		
AWS Lambda	AWS Lambda activité d'exécuti on de fonctions (l'`Invoke`API).	Lambda	`AWS::Lambda::Function`
Amazon S3	Activité de l'API au niveau des objets Amazon S3 (par exemple, `GetObject` `DeleteObj ect` , et opérations d'`PutObject` API) sur des objets dans des compartiments S3.	S3	`AWS::S3::Object`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS AppConfig	AWS AppConfig Activité de l'API pour les opérations de configuration telles que les appels vers `StartConfiguration` `Session` et `GetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Échange de données B2B	Activité de l'API d'échange de données B2B pour les opérations du transformateur telles que les appels vers `GetTransformerJob` et `StartTransformerJob` .	Échange de données B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Activité de l'API Amazon Bedrock sur un alias d'agent.	Alias d'agent Bedrock	`AWS::Bedrock::AgentAlias`
	Activité de l'API Amazon Bedrock sur une base de connaissances.	Base de connaissances Bedrock	`AWS::Bedrock::KnowledgeBase`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon CloudFront	CloudFront Activité de l'API sur un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Activité de l'API sur un espace de noms.	AWS Cloud Map espace de nom	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Activité de l'API sur un service.	AWS Cloud Map web	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` activité sur un chenal CloudTrail lacustre utilisé pour enregistrer des événements provenant de l'extérieur AWS.	CloudTrail canal	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Activité de CodeWhisperer l'API Amazon lors d'une personnalisation.	CodeWhisperer personnalisation	`AWS::CodeWhisperer::Customization`
	Activité de CodeWhisperer l'API Amazon sur un profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Cognito	Activité de l'API Amazon Cognito sur les réserves d'identités Amazon Cognito.	Réserves d'identités Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Activité de l'API Amazon DynamoDB sur les flux.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	API directes Amazon Elastic Block Store (EBS) telles que `PutSnapshotBlock`, `GetSnapshotBlock`, et `ListChangedBlocks` sur des instantanés Amazon EBS.	API directes Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Activité de l'API Amazon EMR sur un espace de travail de journalisation à écriture anticipée.	Espace de travail de journalisation à écriture anticipée EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Activité de l'API Amazon FinSpace sur les environnements.	FinSpace	`AWS::FinSpace::Environment`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS Glue	AWS Glue Activité de l'API sur les tables créées par Lake Formation. **Note** AWS Glue les événements de données pour les tables ne sont actuellement pris en charge que dans les régions suivantes : • USA Est (Virginie du Nord) • USA Est (Ohio) • USA Ouest (Oregon) • Europe (Irlande) • Région Asie-	Lake Formation	`AWS::Glue::Table`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Pacifique (Tokyo)		
Amazon GuardDuty	Activité de GuardDuty l'API Amazon pour un détecteur.	GuardDuty détecteur	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Activité de l'API sur les magasins de données.	Magasin de données d'imagerie médicale	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Activité de l'API sur les certificats.	Certificat IoT	`AWS::IoT::Certificate`
	AWS IoT Activité de l'API sur les objets.	Un truc lié à l'IoT	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	Activité de l'API Greengrass depuis un appareil principal de Greengrass sur une version de composant . **Note** Greengrass n'enregistre pas les cas de refus d'accès.	Version du composant IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de l'API Greengrass depuis un appareil principal de Greengrass lors d'un déploiement. **Note** Greengrass n'enregistre pas les cas de refus d'accès.	Déploiement de Greengrass pour l'IoT	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Activité de SiteWise l'API IoT sur les actifs.	SiteWise Actif IoT	`AWS::IoTSiteWise::Asset`
	Activité de SiteWise l'API IoT sur les séries chronologiques.	Séries SiteWise chronologiques sur l'IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Activité de TwinMaker l'API IoT sur une entité.	TwinMaker Entité IoT	`AWS::IoTTwinMaker::Entity`
	Activité de TwinMaker l'API IoT sur un espace de travail.	Espace de TwinMaker travail IoT	`AWS::IoTTwinMaker::Workspace`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Kendra Intelligent Ranking (Classement intelligent Amazon Kendra)	Activité de l'API de classement intelligent Amazon Kendra sur les plans d'exécution de réévaluation.	Classement Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (pour Apache Cassandra)	Activité de l'API Amazon Keyspaces sur une table.	Table Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	Activité de l'API Kinesis Data Streams sur les flux.	Kinesis Stream	`AWS::Kinesis::Stream`
	Activité de l'API Kinesis Data Streams sur les utilisateurs des streams.	Consommateur de Kinesis Stream	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis	Activité de l'API Kinesis Video Streams sur les flux vidéo, tels que les appels `GetMedia` vers `PutMedia` et.	Flux vidéo Kinesis	`AWS::KinesisVideo::Stream`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Managed Blockchain	Activité de l'API Amazon Managed Blockchain sur un réseau.	Réseau Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Appels Amazon Managed Blockchain JSON-RPC sur les nœuds Ethereum, tels que `eth_getBalance` ou `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Graphe Amazon Neptune	Les activités de l'API de données, par exemple les requêtes, les algorithmes ou la recherche vectoriel le, sur un graphe Neptune.	Graphe Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Connecteur pour l'activité de l'API Active Directory.	AWS Private CA Connecteur pour Active Directory	`AWS::PCAConnectorAD::Connector`
Applications Amazon Q	Activité de l'API de données sur Amazon Q Apps.	Applications Amazon Q	`AWS::QApps:QApp`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Q Business	Activité de l'API Amazon Q Business sur une application.	Application Amazon Q Business	`AWS::QBusiness::Application`
	Activité de l'API Amazon Q Business sur une source de données.	Source de données Amazon Q Business	`AWS::QBusiness::DataSource`
	Activité de l'API Amazon Q Business sur un index.	Indice Amazon Q Business	`AWS::QBusiness::Index`
	Activité de l'API Amazon Q Business dans le cadre d'une expérience Web.	Expérience Web Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Activité de l'API Amazon RDS sur un cluster de base de données.	API de données RDS - Cluster de bases de données	`AWS::RDS::DBCluster`
Amazon S3	Activité de l'API Amazon S3 sur les points d'accès.	Points d'accès S3	`AWS::S3::AccessPoint`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de l'API des points d'accès Amazon S3 Object Lambda, comme les appels vers `CompleteMultipartUpload` et. `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Activité de l'API au niveau de l'objet Amazon S3 on Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Activité d'Amazon sur les terminaux.	SageMaker point final	`AWS::SageMaker::Endpoint`
	Activité de SageMaker l'API Amazon sur les magasins de fonctionnalités.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de SageMaker l'API Amazon sur les composants des essais expérimentaux.	SageMaker composant d'essai expérimental sur les métriques	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Opérations d'API `Publish` d'Amazon SNS sur les points de terminaison de la plateforme.	Point de terminaison de la plateforme SNS	`AWS::SNS::PlatformEndpoint`
	Opérations d'API `Publish` et `PublishBatch` d'Amazon SNS sur des rubriques.	Rubrique SNS	`AWS::SNS::Topic`
Amazon SQS	Activité de l'API Amazon SQS sur les messages.	SQS	`AWS::SQS::Queue`
AWS Step Functions	Activité de l'API Step Functions sur une machine à états.	Machine d'état Step Functions	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain Activité de l'API sur une instance.	Chaîne d'approvisionnement	`AWS::SCN::Instance`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon SWF	Activité de l'API Amazon SWF sur les domaines.	Domaine SWF	`AWS::SWF::Domain`
AWS Systems Manager	Activité de l'API Systems Manager sur les canaux de contrôle.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Activité de l'API Systems Manager sur les nœuds gérés.	Nœud géré par Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Activité de l'API `Query` d'Amazon Timestream sur des bases de données.	Base de données Timestream	`AWS::Timestream::Database`
	Activité de l'API `Query` d'Amazon Timestream sur des tables.	Table Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Activité de l'API Amazon Verified Permissions sur un magasin de politiques.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Activité de l'API Thin Client sur un appareil.	Appareil client léger	`AWS::ThinClient::Device`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	WorkSpaces Activité de l'API Thin Client dans un environnement.	Client léger d'environnement	`AWS::ThinClient::Environment`
AWS X-Ray	Activité de l'API X-Ray sur les traces.	X-Ray Trace	`AWS::XRay::Trace`

Les événements de données ne sont pas journalisés par défaut lorsque vous créez un magasin de données d'événement. Pour enregistrer CloudTrail les événements liés aux données, vous devez ajouter explicitement les ressources prises en charge ou les types de ressources pour lesquels vous souhaitez collecter des activités. Pour plus d'informations sur la journalisation des événements de données, veuillez consulter Journalisation des événements de données.

Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

Événements Insights

CloudTrail Les événements Insights capturent le taux d'appels d'API ou les taux d'erreur inhabituels de votre AWS compte en analysant les activités CloudTrail de gestion. Les événements Insights fournissent des informations pertinentes, telles que l'API associée, le code d'erreur, l'heure de l'incident et les statistiques, ce qui vous aide à comprendre et à agir par rapport à l'activité inhabituelle. Contrairement aux autres types d'événements enregistrés dans un CloudTrail magasin de données de suivi ou d'événements, les événements Insights sont enregistrés uniquement lorsque des modifications sont CloudTrail détectées dans l'utilisation de l'API de votre compte ou dans la journalisation du taux d'erreur qui diffèrent considérablement des modèles d'utilisation habituels du compte.

Voici des exemples d'activité susceptibles de générer des événements Insights :

- Votre compte ne consigne généralement pas plus de 20 appels d'API `DeleteBucket` Amazon S3 par minute, mais commence à consigner une moyenne de 100 appels d'API `DeleteBucket`

par minute. Un événement Insights est enregistré au début de l'activité inhabituelle, et un autre événement Insights est enregistré pour marquer la fin de l'activité inhabituelle.

- Votre compte enregistre généralement 20 appels par minute à l'API `AuthorizeSecurityGroupIngress` Amazon EC2, mais commence à ne consigner aucun appel à `AuthorizeSecurityGroupIngress`. Un événement Insights est enregistré au début de l'activité inhabituelle, et dix minutes plus tard, lorsque l'activité inhabituelle se termine, un autre événement Insights est journalisé pour marquer la fin de l'activité inhabituelle.
- En règle générale, votre compte se connecte à moins d'une erreur `AccessDeniedException` sur une période de sept jours sur AWS Identity and Access Management l'API, `DeleteInstanceProfile`. Votre compte commence à journaliser en moyenne 12 erreurs `AccessDeniedException` par minute sur `DeleteInstanceProfile` l'appel API. Un événement Insights est journalisé au début de l'activité de taux d'erreur inhabituelle, et un autre événement Insights est journalisé pour marquer la fin de l'activité inhabituelle.

Ces exemples sont fournis à titre d'illustration seulement. Vos résultats peuvent varier en fonction de votre cas d'utilisation.

Pour enregistrer les événements CloudTrail Insights, vous devez activer explicitement les événements Insights sur un magasin de données de parcours ou d'événements nouveau ou existant. Pour plus d'informations sur la journalisation des événements Insights, veuillez consulter Journalisation des événements Insights.

Des frais supplémentaires s'appliquent pour les événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.

Affichage des événements Insights pour les sentiers et les magasins de données sur les événements

CloudTrail prend en charge les événements Insights à la fois pour les sentiers et les magasins de données sur les événements, mais il existe certaines différences dans la façon dont vous visualisez et accédez aux événements Insights.

Affichage des événements Insights pour les journaux de suivi

Si les événements Insights sont activés sur un parcours et que vous CloudTrail détectez une activité inhabituelle, les événements Insights sont enregistrés dans un dossier ou un préfixe différent dans le compartiment S3 de destination de votre parcours. Vous pouvez également voir le type d'aperçu et la période de l'incident lorsque vous consultez les événements Insights sur la CloudTrail console. Pour

plus d'informations, consultez Afficher CloudTrail les événements Insights relatifs aux parcours dans la CloudTrail console.

Affichage des événements Insights pour les entrepôts de données d'événement

Pour enregistrer les événements Insights dans CloudTrail Lake, vous avez besoin d'un magasin de données d'événements de destination qui enregistre les événements Insights et d'un magasin de données d'événements source qui active Insights et enregistre les événements de gestion. Pour plus d'informations, consultez Créez un magasin de données d'événements pour les événements CloudTrail Insights à l'aide de la console.

Si CloudTrail Insights est activé sur un magasin de données d'événements source et que vous CloudTrail détectez une activité inhabituelle, CloudTrail transmet les événements Insights à votre magasin de données d'événements de destination. Vous pouvez ensuite interroger votre banque de données d'événements de destination pour obtenir des informations sur vos événements Insights et éventuellement enregistrer les résultats de la requête dans un compartiment S3. Pour plus d'informations, consultez Créer ou modifier une requête et Afficher des exemples de requêtes dans la CloudTrail console.

Vous pouvez consulter le tableau de bord Insights Events pour visualiser les événements Insights dans votre banque de données d'événements de destination. Pour plus d'informations, consultez Afficher les tableaux de bord de CloudTrail Lake.

Historique des événements

CloudTrail l'historique des événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours d'événements de CloudTrail gestion dans un. Région AWS Vous pouvez utiliser cet historique pour obtenir de la visibilité sur les actions effectuées dans votre AWS compte dans les AWS SDK AWS Management Console, les outils de ligne de commande et d'autres AWS services. Vous pouvez personnaliser l'affichage de l'historique des événements dans la CloudTrail console en sélectionnant les colonnes à afficher. Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.

Journaux de suivi

Un suivi est une configuration qui permet de transmettre des CloudTrail événements à un compartiment S3, avec une livraison facultative à CloudWatch Logs et Amazon EventBridge. Vous pouvez utiliser un suivi pour choisir les CloudTrail événements que vous souhaitez diffuser,

chiffrer vos fichiers journaux d' CloudTrail événements à l'aide d'une AWS KMS clé et configurer les notifications Amazon SNS pour la livraison des fichiers journaux. Pour plus d'informations sur la création et la gestion d'un journal de suivi, consultez Création d'un parcours pour votre Compte AWS.

Sentiers multirégionaux et monorégionaux

Vous pouvez créer deux types de sentiers pour un Compte AWS : les sentiers multirégionaux et les sentiers monorégionaux.

Sentiers multirégionaux

Lorsque vous créez un journal multirégional, enregistrez CloudTrail les événements dans l'ensemble Régions AWS de la AWS partition sur laquelle vous travaillez et délivre les fichiers journaux d' CloudTrail événements dans un compartiment S3 que vous spécifiez. Si un Région AWS est ajouté après avoir créé un parcours multirégional, cette nouvelle région est automatiquement incluse et les événements de cette région sont enregistrés. La création d'un journal de suivi multi-régions est une bonne pratique recommandée, car vous pouvez journaliser l'activité dans toutes les régions dans votre compte. Tous les sentiers que vous créez à l'aide de la CloudTrail console sont multirégionaux. Vous pouvez convertir un parcours à région unique en un parcours multirégional à l'aide du. AWS CLI Pour plus d'informations, consultez Créer un journal de suivi dans la console et Convertir un journal de suivi qui s'applique à une région de sorte qu'il s'applique à toutes les régions.

Sentiers d'une seule région

Lorsque vous créez un parcours d'une seule région, CloudTrail enregistre les événements de cette région uniquement. Il fournit ensuite les fichiers journaux d' CloudTrail événements à un compartiment Amazon S3 que vous spécifiez. Vous ne pouvez créer un journal de suivi à région unique qu'à l'aide de l' AWS CLI. Si vous créez des pistes uniques supplémentaires, vous pouvez faire en sorte que ces pistes fournissent des fichiers journaux d' CloudTrail événements dans le même compartiment S3 ou dans des compartiments séparés. Il s'agit de l'option par défaut lorsque vous créez un parcours à l'aide de l'API AWS CLI ou de l' CloudTrail API. Pour plus d'informations, consultez Création, mise à jour et gestion de sentiers à l'aide du AWS CLI.

> **Note**
>
> Pour les deux types de journaux de suivi, vous pouvez spécifier un compartiment Amazon S3 de n'importe quelle région.

Un sentier multirégional présente les avantages suivants :

- Les paramètres de configuration du sentier s'appliquent de manière cohérente à tous Régions AWS.
- Vous recevez les CloudTrail événements de tous Régions AWS dans un seul compartiment Amazon S3 et, éventuellement, dans un groupe de CloudWatch journaux Logs.
- Vous gérez la configuration des sentiers pour tous Régions AWS à partir d'un seul endroit.

Lorsque vous appliquez une piste à toutes les AWS régions, CloudTrail utilisez la piste que vous créez dans une région particulière pour créer des pistes avec des configurations identiques dans toutes les autres régions de la AWS partition dans laquelle vous travaillez.

Cela a les effets suivants :

- CloudTrail fournit des fichiers journaux pour l'activité du compte provenant de toutes les AWS régions vers le compartiment Amazon S3 unique que vous spécifiez et, éventuellement, vers un groupe de CloudWatch journaux de journaux.
- Si vous avez configuré une rubrique Amazon SNS pour le suivi, les notifications SNS concernant les livraisons de fichiers journaux dans toutes les AWS régions sont envoyées à cette rubrique SNS unique.

Qu'il s'agisse d'un parcours multirégional ou mono-régional, les événements envoyés à Amazon EventBridge sont reçus dans le bus d'événements de chaque région, plutôt que dans un seul bus d'événements.

Plusieurs journaux de suivi par région

Si vous avez des groupes d'utilisateurs différents mais associés, comme des développeurs, du personnel de sécurité et des auditeurs informatiques, vous pouvez créer plusieurs journaux de suivi par région. Cela permet à chaque groupe de recevoir son propre exemplaire des fichiers journaux.

CloudTrail prend en charge cinq sentiers par région. Un sentier multirégional compte pour un sentier par région.

Voici un exemple de région comportant cinq sentiers :

- Vous créez deux journaux de suivi dans la région USA Ouest (Californie du Nord) qui s'appliquent uniquement à cette région.

- Vous créez deux autres sentiers multirégionaux dans la région de l'ouest des États-Unis (Californie du Nord).
- Vous créez un autre parcours multirégional dans la région Asie-Pacifique (Sydney). Ce journal de suivi existe aussi comme journal de suivi dans la région USA Ouest (Californie du Nord).

Vous pouvez consulter la liste des sentiers Région AWS dans une page des sentiers de la CloudTrail console. Pour plus d'informations, consultez Mise à jour d'un journal de suivi. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

Sentiers d'organisation

Un suivi d'organisation est une configuration qui permet de transférer les CloudTrail événements du compte de gestion et de tous les comptes membres d'une AWS Organizations organisation vers le même compartiment Amazon S3, CloudWatch les mêmes journaux et Amazon EventBridge. La création d'un journal de suivi d'organisation vous permet de définir une stratégie de journalisation des événements uniforme pour votre organisation.

Tous les parcours d'organisation créés à l'aide de la console sont des journaux d'organisation multirégionaux qui enregistrent les événements associés aux comptes activés Régions AWS dans chaque compte membre de l'organisation. Pour enregistrer les événements dans toutes les AWS partitions de votre organisation, créez un journal d'organisation multirégional dans chaque partition. Vous pouvez créer un journal d'organisation à région unique ou multirégionale à l'aide du. AWS CLI Si vous créez un sentier à région unique, vous enregistrez l'activité uniquement dans le sentier Région AWS (également appelé région d'origine).

Bien que la plupart Régions AWS soient activées par défaut pour vous Compte AWS, vous devez activer manuellement certaines régions (également appelées régions optionnelles). Pour plus d'informations sur les régions activées par défaut, consultez la section Considérations relatives à l'activation et à la désactivation des régions dans le Guide de AWS Account Management référence. Pour la liste des régions prises CloudTrail en charge, voirCloudTrail Régions prises en charge.

Lorsque vous créez un historique d'organisation, une copie du journal portant le nom que vous lui donnez est créée dans les comptes des membres appartenant à votre organisation.

- Si le parcours de l'organisation concerne une seule région et que la région d'origine du sentier n'est pas une région OPT, une copie du parcours est créée dans la région d'origine du parcours de l'organisation dans chaque compte membre.

- Si le parcours de l'organisation concerne une seule région et que la région d'origine du sentier est une région OPT, une copie du parcours est créée dans la région d'origine du parcours de l'organisation sur les comptes des membres qui ont activé cette région.
- Si le parcours de l'organisation est multirégional et que la région d'origine du sentier n'est pas une région optionnelle, une copie du parcours est créée dans chaque région activée Région AWS dans chaque compte membre. Lorsqu'un compte membre active une région optionnelle, une copie du parcours multirégional est créée dans la région nouvellement inscrite pour le compte du membre une fois l'activation de cette région terminée.
- Si le parcours de l'organisation est multirégional et que la région d'origine est une région optionnelle, les comptes membres n'enverront aucune activité au parcours de l'organisation à moins qu'ils n'aient choisi celui Région AWS où le parcours multirégional a été créé. Par exemple, si vous créez un parcours multirégional et que vous choisissez la région Europe (Espagne) comme région d'origine du parcours, seuls les comptes membres ayant activé la région Europe (Espagne) pour leur compte enverront l'activité de leur compte au parcours de l'organisation.

> **Note**
>
> CloudTrail crée des traces d'organisation dans les comptes des membres même en cas d'échec de la validation des ressources. Voici des exemples d'échecs de validation :
>
> - une politique de compartiment Amazon S3 incorrecte
> - une politique de rubrique Amazon SNS incorrecte
> - impossibilité de livrer à un groupe de CloudWatch journaux Logs
> - autorisation insuffisante pour chiffrer à l'aide d'une clé KMS
>
> Un compte membre disposant d' CloudTrail autorisations peut voir les échecs de validation d'un journal d'organisation en consultant la page de détails du journal sur la CloudTrail console ou en exécutant la AWS CLI get-trail-statuscommande.

Les utilisateurs autorisés CloudTrail à accéder aux comptes membres pourront consulter le parcours de l'organisation (y compris l'ARN du journal) lorsqu'ils se connectent à la AWS CloudTrail console depuis leur AWS compte ou lorsqu'ils exécutent des AWS CLI commandes telles que `describe-trails` (bien que les comptes membres doivent utiliser l'ARN pour le suivi de l'organisation, et non le nom, lorsqu'ils utilisent le AWS CLI). Toutefois, les utilisateurs des comptes membres ne

disposeront pas des autorisations suffisantes pour supprimer les traces de l'organisation, activer ou désactiver la connexion, modifier les types d'événements enregistrés ou modifier de quelque manière que ce soit les traces de l'organisation. Pour plus d'informations sur AWS Organizations, consultez Terminologie et concepts Organizations. Pour plus d'informations sur la création et l'utilisation de journaux de suivi de l'organisation, consultez Création d'un journal de suivi pour une organisation.

CloudTrail Magasins de données sur les lacs et les événements

CloudTrail Lake vous permet d'exécuter des requêtes SQL précises sur vos événements et de consigner les événements provenant de sources extérieures AWS, notamment de vos propres applications et de partenaires intégrés à ces derniers. CloudTrail Il n'est pas nécessaire de configurer un sentier dans votre compte pour utiliser CloudTrail Lake.

Les événements sont agrégés dans des magasins de données d'événement, qui sont des ensembles inaltérables d'événements basés sur des critères que vous sélectionnez en appliquant les sélecteurs d'événements avancés. Vous pouvez conserver les données d'événement dans une banque de données d'événement jusqu'à 3 653 jours (environ 10 ans) si vous choisissez l'option de tarification de rétention extensible d'un an, ou jusqu'à 2 557 jours (environ 7 ans) si vous choisissez l'option de tarification de rétention de sept ans. Vous pouvez enregistrer les requêtes Lake pour une utilisation ultérieure et afficher les résultats des requêtes pendant sept jours au maximum. Vous pouvez également enregistrer les résultats des requêtes dans un compartiment S3. CloudTrail Lake peut également stocker les événements d'une organisation AWS Organizations dans un magasin de données d'événements, ou les événements provenant de plusieurs régions et comptes. CloudTrail Lake fait partie d'une solution d'audit qui vous aide à effectuer des enquêtes de sécurité et à résoudre des problèmes. Pour plus d'informations, consultez Travailler avec AWS CloudTrail Lake et CloudTrail Concepts et terminologie relatifs aux lacs.

CloudTrail Perspectives

CloudTrail Insights aide AWS les utilisateurs à identifier et à répondre aux volumes inhabituels d'appels d'API ou aux erreurs enregistrées lors des appels d'API en analysant en permanence les événements CloudTrail de gestion. Un événement Insights est un registre de niveaux inhabituels de l'activité de l'API de gestion `write` ou niveaux inhabituels d'erreurs renvoyés lors de l'activité de l'API de gestion. Par défaut, les magasins de données de parcours et d'événements n'enregistrent pas les événements CloudTrail Insights. Dans la console, vous pouvez choisir de journaliser les événements Insights lorsque vous créez ou mettez à jour un journal de suivi ou un entrepôt de données d'événement. Lorsque vous utilisez l' CloudTrail API, vous pouvez enregistrer les événements Insights en modifiant les paramètres d'un magasin de données de suivi ou d'événement

existant à l'aide de l'`PutInsightSelectors`API. Des frais supplémentaires s'appliquent pour la journalisation CloudTrail des événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, veuillez consulter les sections Journalisation des événements Insights et Tarification d'AWS CloudTrail.

Balises

Une balise est une clé définie par le client et une valeur facultative qui peuvent être attribuées à AWS des ressources, telles que les CloudTrail parcours, les magasins de données d'événements et les canaux, les compartiments S3 utilisés pour stocker les fichiers CloudTrail journaux, les AWS Organizations organisations et les unités organisationnelles, etc. En ajoutant les mêmes balises aux sentiers et aux compartiments S3 que vous utilisez pour stocker les fichiers journaux des sentiers, vous pouvez faciliter la gestion, la recherche et le filtrage de ces ressources. AWS Resource Groups Vous pouvez mettre en œuvre des stratégies d'étiquette pour vous aider à trouver et gérer vos ressources uniformément, efficacement et facilement. Pour plus d'informations, consultez la section Meilleures pratiques en matière de balisage AWS des ressources.

AWS Security Token Service et CloudTrail

AWS Security Token Service (AWS STS) est un service doté d'un point de terminaison global et prenant également en charge les points de terminaison spécifiques à une région. Un point de terminaison est une URL qui constitue le point d'entrée des demandes de service Web. Par exemple, `https://cloudtrail.us-west-2.amazonaws.com` est le point d'entrée régional du AWS CloudTrail service dans l'ouest des États-Unis (Oregon). Les points de terminaison régionaux aident à réduire la latence dans vos applications.

Lorsque vous utilisez un point de AWS STS terminaison spécifique à une région, le parcours de cette région fournit uniquement les AWS STS événements qui se produisent dans cette région. Par exemple, si vous utilisez le point de terminaison `sts.us-west-2.amazonaws.com`, le journal de suivi de la région us-west-2 fournit uniquement les événements AWS STS provenant de la région us-west-2. Pour plus d'informations sur les points de terminaison AWS STS régionaux, consultez la section Activation et désactivation AWS STS dans une AWS région dans le guide de l'utilisateur IAM.

Pour une liste complète des points de terminaison AWS régionaux, voir AWS Régions et points de terminaison dans le. Références générales AWS Pour plus de détails sur les événements de points de terminaison AWS STS mondiaux, consultez Événements de services mondiaux.

Événements de services mondiaux

> **Important**
>
> Depuis le 22 novembre 2021, la façon dont les sentiers capturent les événements liés au service mondial AWS CloudTrail a changé. Désormais, les événements créés par Amazon CloudFront AWS STS sont enregistrés dans la région dans laquelle ils ont été créés, la région USA Est (Virginie du Nord), us-east-1. AWS Identity and Access Management Cela rend le CloudTrail traitement de ces services cohérent avec celui des autres services AWS mondiaux. Pour continuer à recevoir les événements de service global en dehors des USA Est (Virginie du Nord), veillez à convertir les journaux de suivi à région unique utilisant des événements de services mondiaux en dehors des USA Est (Virginie du Nord) en journaux de suivi multi-régions. Pour plus d'informations sur la capture des événements de services mondiaux, consultez Activation et désactivation de la journalisation des événements de services mondiaux plus loin dans cette section.
> En revanche, l'historique des événements de la CloudTrail console et la aws cloudtrail lookup-events commande afficheront ces événements Région AWS là où ils se sont produits.

Pour la plupart des services, les événements sont enregistrés dans la région où l'action s'est produite. Pour les services internationaux tels que AWS Identity and Access Management (IAM) et Amazon AWS STS CloudFront, les événements sont organisés sur tous les parcours qui incluent des services mondiaux.

Pour la plupart des services mondiaux, les événements sont journalisés comme s'ils se produisaient dans la région USA Est (Virginie du Nord), mais certains événements de service mondiaux sont journalisés comme s'ils se produisaient dans d'autres régions, comme la région USA Est (Ohio) ou la région USA Ouest (Oregon).

Pour éviter de recevoir des doublons d'événements de services globaux, n'oubliez pas les points suivants :

- Les événements de service globaux sont transmis par défaut aux pistes créées à l'aide de la CloudTrail console. Les événements sont livrés au compartiment pour le journal de suivi.
- Si vous avez plusieurs journaux de suivi sur une seule région, pensez à configurer vos journaux de suivi de manière à ce que les événements de services mondiaux soient diffusés dans un seul des journaux de suivi. Pour plus d'informations, consultez Activation et désactivation de la journalisation des événements de services mondiaux.

- Si vous modifiez la configuration d'un journal de suivi afin qu'il s'applique à une région unique au lieu de s'appliquer à toutes les régions, la journalisation des événements de services mondiaux est désactivée automatiquement pour ce journal de suivi. De la même manière, si vous modifiez la configuration d'un journal de suivi afin qu'il s'applique à toutes les régions au lieu de s'appliquer à une région unique, la journalisation des événements de services mondiaux est activée automatiquement pour ce journal de suivi.

  Pour plus d'informations sur la modification de la journalisation des événements de services mondiaux pour un journal de suivi, consultez Activation et désactivation de la journalisation des événements de services mondiaux.

Exemple :

1. Vous créez un parcours dans la CloudTrail console. Par défaut, ce journal de suivi consigne les événements de services mondiaux.
2. Vous avez plusieurs journaux de suivi à région unique.
3. Vous n'avez pas besoin d'inclure les services globaux pour les suivis à une région unique. Les événements de services mondiaux sont fournis pour le premier journal de suivi. Pour plus d'informations, consultez Création, mise à jour et gestion de sentiers à l'aide du AWS CLI.

> **Note**
>
> Lorsque vous créez ou mettez à jour un parcours à l' AWS CLI aide AWS des SDK ou de l' CloudTrail API, vous pouvez spécifier s'il convient d'inclure ou d'exclure les événements de service globaux pour les sentiers. Vous ne pouvez pas configurer la journalisation globale des événements de service depuis la CloudTrail console.

CloudTrail Régions prises en charge

> **Note**
>
> Pour plus d'informations sur les régions prises en charge par CloudTrail Lake, consultezCloudTrail Régions soutenues par les lacs.
> Pour plus d'informations sur les extrémités du plan de données, consultez la section Points de terminaison du plan de données dans le. Références générales AWS

Nom de la région	Région	Point final du plan de contrôle	Protocole	Date de la prise en charge
USA Est (Virginie du Nord)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	13/11/2013
USA Est (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	17-10-2016
USA Ouest (Californie du Nord)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	13/05/2014
USA Ouest (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	13/11/2013
Afrique (Le Cap)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	22/04/2020
Asie-Pacifique (Hong Kong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	24/04/2019
Asie-Pacifique (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	22/11/2022
Asie-Pacifique (Jakarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	13/12/2021
Asie-Pacifique (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	23/01/2023

Nom de la région	Région	Point final du plan de contrôle	Protocole	Date de la prise en charge
Asie-Pacifique (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	27/06/2016
Asie-Pacifique (Osaka)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	12/02/2018
Asie-Pacifique (Séoul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	06/01/2016
Asie-Pacifique (Singapour)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	30/06/2014
Asie-Pacifique (Sydney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	13/05/2014
Asie-Pacifique (Tokyo)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	30/06/2014
Canada (Centre)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	12/08/2016
Canada Ouest (Calgary)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	20/12/2023
Chine (Beijing)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	01/03/2014

Nom de la région	Région	Point final du plan de contrôle	Protocole	Date de la prise en charge
Chine (Ningxia)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	12/11/2017
Europe (Francfort)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	23/10/2014
Europe (Irlande)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	13/05/2014
Europe (Londres)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	12/13/2016
Europe (Milan)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	27/04/2020
Europe (Paris)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	12/18/2017
Europe (Espagne)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	16/11/2022
Europe (Stockholm)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	12-11-2018
Europe (Zurich)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
Israël (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	31 JUILLET 2023
Moyen-Orient (Bahreïn)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	29/07/2019

Nom de la région	Région	Point final du plan de contrôle	Protocole	Date de la prise en charge
Moyen-Orient (EAU)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	30/08/2022
Amérique du Sud (São Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	30/06/2014
AWS GovCloud (USA Est)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	12/11/2018
AWS GovCloud (US-Ouest)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	16/08/2011

Pour plus d'informations sur l'utilisation CloudTrail dans le AWS GovCloud (US) Regions, consultez la section Points de terminaison du service dans le guide de l'AWS GovCloud (US) utilisateur.

Pour plus d'informations sur l'utilisation CloudTrail dans la région de Chine (Pékin), consultez la section Points de terminaison et ARN pour la Chine AWS dans le. Référence générale d'Amazon Web Services

CloudTrail services et intégrations pris en charge

CloudTrail prend en charge la journalisation des événements pour de nombreuses personnes Services AWS. Vous trouverez des détails pour chaque service pris en charge dans le guide de ce service. Pour obtenir la liste des sujets spécifiques aux services, consultez. AWS sujets de service pour CloudTrail En outre, certains Services AWS peuvent être utilisés pour analyser et agir sur les données collectées dans CloudTrail les journaux.

> **Note**
>
> Pour voir la liste des régions prises en charge pour chaque service, veuillez consulter Service endpoints and quotas dans la Référence générale d'Amazon Web Services.

Rubriques

AWS intégrations de services avec journaux CloudTrail

> **Note**
>
> Vous pouvez également utiliser CloudTrail Lake pour interroger et analyser vos événements. CloudTrail Les requêtes Lake offrent une vue plus approfondie et plus personnalisable des événements que de simples recherches de clés et de valeurs dans l'historique des événements ou en cours d'exécution`LookupEvents`. CloudTrail Les utilisateurs de Lake peuvent exécuter des requêtes SQL (Standard Query Language) complexes sur plusieurs champs lors d'un CloudTrail événement. Pour plus d'informations, consultez Travailler avec AWS CloudTrail Lake et Copier les événements du sentier sur CloudTrail le lac.
> CloudTrail Les stockages et requêtes de données sur les événements de Lake sont payants CloudTrail . Pour plus d'informations sur la tarification des CloudTrail lacs, consultez la section AWS CloudTrail Tarification.

Vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les rubriques suivantes.

AWS Service	Rubrique	Description
Amazon Athena	Journaux d'interrogation AWS CloudTrail	L'utilisation d'Athena avec CloudTrail les journaux est un moyen efficace d'améliorer votre analyse de l'activité des AWS services. Par exemple, vous pouvez utiliser des requêtes pour identifier des tendances et isoler davantage l'activité par attribut, comme l'adresse IP source ou l'utilisateur. Vous pouvez créer automatiquement des tables pour interroger les journaux directement depuis la CloudTrail console et utiliser ces tables pour exécuter des requêtes dans Athena. Pour plus d'informations, consultez la section Création d'une table pour les CloudTrail journaux dans la CloudTrail console dans le guide de l'utilisateur d'Amazon Athena. **Note** L'exécution de requêtes dans Amazon Athena génère des coûts supplémentaires. Pour plus d'informations,

AWS Service	Rubrique	Description
		consultez Tarification Amazon Athena.
Amazon CloudWatch Logs	Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs	Vous pouvez configurer CloudTrail les CloudWatch journaux pour surveiller vos journaux de suivi et être averti lorsqu'une activité spécifique se produit. Par exemple, vous pouvez définir CloudWatc h des filtres métriques de Logs qui déclencheront des CloudWatch alarmes et vous enverront des notifications lorsque ces alarmes sont déclenchées. **Note** La tarification standard pour Amazon CloudWatch et Amazon CloudWatc h Logs s'applique. Pour en savoir plus, consultez Tarification Amazon CloudWatch .

CloudTrail intégration avec Amazon EventBridge

Amazon EventBridge est un AWS service qui fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux AWS ressources. Dans EventBridge, vous pouvez

créer des règles qui répondent aux événements enregistrés par CloudTrail. Pour plus d'informations, consultez Créer une règle sur Amazon EventBridge.

Vous pouvez diffuser les événements auxquels vous êtes abonné sur votre parcours EventBridge en créant une règle avec la EventBridge console.

Depuis la EventBridge console :

- Choisissez le `AWS API Call via CloudTrail` type de détail pour transmettre les CloudTrail données et les événements de gestion avec un `eventType` de. `AwsApiCall` Pour enregistrer des événements dont la valeur de type détaillé est égale à`AWS API Call via CloudTrail`, vous devez disposer d'une trace qui enregistre actuellement des événements de gestion ou de données.
- Choisissez le `AWS Console Sign In via CloudTrail` type de détail pour organiser les événements de AWS Management Console connexion. Pour enregistrer des événements avec un type de détail de`AWS Console Sign In via CloudTrail`, vous devez disposer d'un journal qui enregistre actuellement les événements de gestion.
- Choisissez le `AWS Insight via CloudTrail` type de détail pour diffuser des événements Insights. Pour enregistrer des événements dont la valeur de type détaillé est égale à`AWS Insight via CloudTrail`, vous devez disposer d'un historique qui enregistre actuellement les événements Insights. Pour plus d'informations sur la journalisation des événements Insights, veuillez consulter Journalisation des événements Insights.

Pour en savoir plus sur la création d'un journal de suivi, veuillez consulter Création d'un journal de suivi.

CloudTrail intégration avec AWS Organizations

Le compte de gestion d'une AWS Organizations organisation peut ajouter un administrateur délégué pour gérer les CloudTrail ressources de l'organisation. Vous pouvez créer un journal de suivi d'organisation ou un entrepôt de données d'événement d'organisation dans le compte de gestion ou le compte d'administrateur délégué d'une organisation qui collecte toutes les données d'événements pour tous les comptes AWS d'une organisation dans AWS Organizations. La création d'un journal de suivi d'organisation vous permet de définir une stratégie de journalisation des événements uniforme pour votre organisation.

Un suivi de l'organisation est automatiquement appliqué à chaque AWS compte de votre organisation. Les utilisateurs de comptes membres peuvent voir ces journaux de suivi, mais ne peuvent pas les modifier, et par défaut ne peuvent pas afficher les fichiers journaux créés pour le

journal de suivi de l'organisation. Pour plus d'informations, consultez Création d'un journal de suivi pour une organisation.

AWS sujets de service pour CloudTrail

Vous pouvez en savoir plus sur la façon dont les événements relatifs à AWS des services individuels sont enregistrés dans CloudTrail des journaux, notamment des exemples d'événements relatifs à ce service dans des fichiers journaux. Pour plus d'informations sur la manière dont AWS des services spécifiques s'intègrent CloudTrail, consultez la rubrique relative à l'intégration dans le guide individuel de chaque service.

Les services qui sont encore en version préliminaire, qui ne sont pas encore disponibles pour une mise à disposition générale (GA) ou qui ne disposent pas d'API publiques ne sont pas considérés comme pris en charge. CloudTrail ne consigne actuellement pas les événements spécifiques à la politique des points de terminaison Amazon VPC.

> **Note**
>
> Pour voir la liste des régions prises en charge pour chaque service, veuillez consulter Service endpoints and quotas dans la Référence générale d'Amazon Web Services.
> Pour plus d'informations sur les services qui enregistrent les événements de données, veuillez consulter Événements de données.

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon API Gateway	Enregistrez les appels de gestion des API vers Amazon API Gateway à l'aide de AWS CloudTrail	09/07/2015
Amazon AppFlow	Journalisation des appels AppFlow d'API Amazon avec AWS CloudTrail	22/04/2020
Amazon AppStream 2.0	Journalisation des appels d'API Amazon AppStream 2.0 avec AWS CloudTrail	25/04/2019

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Athena	Journalisation des appels d'API Amazon Athena avec AWS CloudTrail	19/05/2017
Amazon Aurora	Surveillance des appels d'API Amazon Aurora AWS CloudTrail	31 août 2018
Amazon Bedrock	Enregistrez les appels d'API Amazon Bedrock en utilisant AWS CloudTrail	23/10/2023
Amazon Braket	Connexion à l'API Amazon Braket avec CloudTrail	08/12/2020
Amazon Chime	Enregistrez les appels d'administration d'Amazon Chime en utilisant AWS CloudTrail	27/09/2017
Amazon Cloud Directory	Journalisation des appels d'API Cloud Directory à l'aide AWS CloudTrail	26/01/2017
Amazon CloudFront	Utilisation AWS CloudTrail pour capturer les demandes envoyées à l' CloudFront API	28/05/2014
Amazon CloudSearch	Journalisation des appels CloudSearch du service de configuration Amazon à l'aide de AWS CloudTrail	16/10/2014
Amazon CloudWatch	Enregistrement des appels CloudWatch d'API Amazon AWS CloudTrail	30/04/2014

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon CloudWatch Logs	Enregistrement des appels CloudWatch d'API Amazon Logs AWS CloudTrail	10/03/2016
Amazon CodeCatalyst	Enregistrement des appels CodeCatalyst d'API en mode connecté à Comptes AWS l'aide de AWS CloudTrail	01/12/2022
CodeGuru Réviseur Amazon	Journalisation des appels d'API Amazon CodeGuru Reviewer avec AWS CloudTrail	02/12/2019
Amazon CodeWhisperer	AWS CloudTrail et CodeWhisperer APIs	13/04/2023
Amazon Cognito	Journalisation des appels d'API Amazon Cognito avec AWS CloudTrail	18/02/2016
Amazon Comprehend	Journalisation des appels d'API Amazon Comprehend avec AWS CloudTrail	17/01/2018
Amazon Comprehend Medical	Journalisation des appels d'API Amazon Comprehend Medical à l'aide d' AWS CloudTrail	11-27-2018
Amazon Connect	Journalisation des appels d'API Amazon Connect à l'aide d' AWS CloudTrail	12/11/2019
Amazon Data Firehose	Surveillance des appels d'API Amazon Data Firehose avec AWS CloudTrail	17/03/2016

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Data Lifecycle Manager	Journalisation des appels d'API Amazon Data Lifecycle Manager à l'aide de AWS CloudTrail	24/07/2018
Amazon Detective	Journalisation des appels d'API Amazon Detective à l'aide d' AWS CloudTrail	31 MARS 2020
Amazon DevOps Guru	Journalisation des appels d'API Amazon DevOps Guru avec AWS CloudTrail	04/05/2021
Amazon DocumentDB (compatible avec MongoDB)	Journalisation des appels d'API Amazon DocumentDB à l'aide d' AWS CloudTrail	09/01/2019
Amazon DynamoDB	Journalisation des opération s DynamoDB à l'aide de AWS CloudTrail	28/05/2015
Amazon EC2	Enregistrez les appels d'API Amazon EC2 à l'aide de AWS CloudTrail	13/11/2013
Amazon EC2 Auto Scaling	Journalisation des appels d'API Auto Scaling en utilisant CloudTrail	16/07/2014
Amazon EC2 Capacity Blocks	La capacité de journalisation bloque les appels d'API avec AWS CloudTrail	31 OCTOBRE 2023
Amazon EC2 Image Builder	Journalisation des appels d'API EC2 Image Builder à l'aide de CloudTrail	02/12/2019

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Elastic Block Store (Amazon EBS) API directes EBS	Journalisation des appels d'API à l'aide AWS CloudTrail Journaliser les appels d'API directes EBS avec AWS CloudTrail	Amazon EBS : 13/11/2013 API directes EBS : 30/06/2020
Amazon Elastic Container Registry (Amazon ECR)	Journalisation des appels d'API Amazon ECR en utilisant AWS CloudTrail	21/12/2015
Amazon Elastic Container Service (Amazon ECS)	Journalisation des appels d'API Amazon ECS en utilisant AWS CloudTrail	09/04/2015
Amazon Elastic File System (Amazon EFS)	Journalisation des appels d'API Amazon EFS avec AWS CloudTrail	28/06/2016
Amazon Elastic Kubernetes Service (Amazon EKS)	Journalisation des appels d'API Amazon EKS avec AWS CloudTrail	05/06/2018
Amazon Elastic Transcoder	Journalisation des appels d'API Amazon Elastic Transcoder avec AWS CloudTrail	27/10/2014
Amazon ElastiCache	Journalisation des appels ElastiCache d'API Amazon à l'aide AWS CloudTrail	15/09/2014
Amazon EMR	Enregistrement des appels d'API Amazon EMR AWS CloudTrail	04/04/2014

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon EMR sur EKS	Journalisation des appels d'API Amazon EMR sur EKS à l'aide d' AWS CloudTrail	09/12/2020
Amazon EventBridge	Journalisation des appels d' EventBridge API Amazon à l'aide de AWS CloudTrail	07/11/2019
Amazon FinSpace	Journaux d'interrogation AWS CloudTrail	18 octobre 2022
Amazon Forecast	Journalisation des appels d'API Amazon Forecast avec AWS CloudTrail	11-28-2018
Amazon Fraud Detector	Journalisation des appels d'API Amazon Fraud Detector à l'aide d' AWS CloudTrail	01/09/2020
Amazon FSx pour Lustre	Journalisation des appels d'API Amazon FSx for Lustre avec AWS CloudTrail	11/01/2019
Amazon FSx for Windows File Server	Surveillance avec AWS CloudTrail	11-28-2018
Amazon GameLift	Journalisation des appels GameLift d'API Amazon avec AWS CloudTrail	27/01/2016
Amazon GuardDuty	Journalisation des appels GuardDuty d'API Amazon avec AWS CloudTrail	12/02/2018
Amazon Inspector	Journalisation des appels d'API Amazon Inspector à l'aide de AWS CloudTrail	29/11/2021

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Inspector Classic	Journalisation des appels d'API Amazon Inspector Classic avec AWS CloudTrail	20/04/2016
Tous les scans Amazon Inspector	Informations relatives à Amazon Inspector Scan dans CloudTrail	27/11/2023
Amazon Interactive Video Service	Journalisation des appels d'API Amazon IVS avec AWS CloudTrail	15/07/2020
Amazon Kendra	Journalisation des appels de l'API Amazon Kendra AWS CloudTrail et journalisation des appels de l'API Amazon Kendra Intelligent Ranking avec des journaux AWS CloudTrail	05/11/2020
Amazon Keyspaces (pour Apache Cassandra)	Journalisation des appels d'API Amazon Keyspaces à l'aide d' AWS CloudTrail	13/01/2020
Service géré Amazon pour Apache Flink	Service géré de journalisation pour les appels d'API Apache Flink avec AWS CloudTrail	22/03/2019
Amazon Kinesis Data Streams	Journalisation des appels d'API Amazon Kinesis Data Streams à l'aide de AWS CloudTrail	25/04/2014
Amazon Kinesis Video Streams	Enregistrement des appels d'API Kinesis Video Streams avec AWS CloudTrail	24/05/2018

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Lex	Journalisation des appels d'API Amazon Lex avec CloudTrail	15/08/2017
Amazon Lightsail	Journalisation des appels d'API Lightsail avec AWS CloudTrail	23/12/2016
Amazon Location Service	Journalisation et surveillance à l'aide d' AWS CloudTrail	15 décembre 2020
Amazon Lookout for Equipment	Surveillance d'Amazon Lookout for Equipment	01/12/2020
Amazon Lookout for Metrics	Affichage de l'activité de l'API Amazon Lookout for Metrics dans AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	Journalisation des appels Amazon Lookout for Vision à l'aide d' AWS CloudTrail	01/12/2020
Amazon Machine Learning	Journalisation des appels d'API Amazon ML en utilisant AWS CloudTrail	10/12/2015
Amazon Macie	Journaliser les appels d'API Amazon Macie à l'aide d' AWS CloudTrail	13/05/2020

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Managed Blockchain	Journalisation des appels d'API Amazon Managed Blockchain à l'aide d' AWS CloudTrail Journalisation d'Ethereum pour les appels d'API Managed Blockchain à l'aide de AWS CloudTrail (Prévisualiser)	01/04/2019
Amazon Managed Grafana	Journalisation des appels d'API Amazon Managed Grafana à l'aide d' AWS CloudTrail	15 décembre 2020
Amazon Managed Service for Prometheus	Journalisation Amazon Managed Service pour les appels d'API Prometheus à l'aide d' AWS CloudTrail	15 décembre 2020
Amazon Managed Streaming for Apache Kafka	Journalisation des appels d'API avec AWS CloudTrail	12-11-2018
Amazon Managed Workflows for Apache Airflow	Afficher les journaux d'audit AWS CloudTrail	24/11/2020
Amazon MemoryDB for Redis	Journalisation des appels d'API Amazon MemoryDB pour Redis avec AWS CloudTrail	19/08/2021
Amazon MQ	Journalisation des appels d'API Amazon MQ à l'aide de AWS CloudTrail	19/07/2018

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Neptune	Journalisation des appels d'API Amazon Neptune à l'aide de AWS CloudTrail	30/05/2018
Amazon Nimble Studio	Enregistrement des appels Nimble Studio à l'aide de AWS CloudTrail	19/06/2023
Amazon One Enterprise	Journalisation des appels d'API Amazon One Enterprise à l'aide de AWS CloudTrail	27/11/2023
Amazon OpenSearch Service	Surveillance des appels OpenSearch d'API Amazon Service avec AWS CloudTrail	01/10/2015
Amazon Personalize	Journalisation des appels d'API Amazon Personalize avec AWS CloudTrail	11-28-2018
Amazon Pinpoint	Journalisation des appels d'API Amazon Pinpoint avec AWS CloudTrail	06/02/2018
API SMS et voix Amazon Pinpoint	Journalisation des appels d'API Amazon Pinpoint avec AWS CloudTrail	11-16-2018
Amazon Polly	Journalisation des appels d'API Amazon Polly avec AWS CloudTrail	30/11/2016
Amazon Q (pour un usage professionnel)	Journalisation des appels d'API Amazon Q à l'aide de AWS CloudTrail	28/11/2023

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Q (à l'usage des AWS constructeurs)	Journalisation des appels d'API Amazon Q à l'aide de AWS CloudTrail	28/11/2023
Amazon Quantum Ledger Database (Amazon QLDB)	Journalisation des appels d'API Amazon QLDB à l'aide d' AWS CloudTrail	10/09/2019
Amazon QuickSight	Opérations de journalisation avec CloudTrail	28/04/2017
Amazon Relational Database Service (Amazon RDS)	Journalisation des appels d'API Amazon RDS à l'aide de AWS CloudTrail	13/11/2013
Analyse des performances d'Amazon RDS	Journalisation des appels d'API Amazon RDS à l'aide de AWS CloudTrail L'API Amazon RDS Performance Insights est un sous-ensemble de l'API Amazon RDS.	21/06/2018
Amazon Redshift	Journalisation des appels d'API Amazon Redshift avec AWS CloudTrail	10/06/2014
Amazon Rekognition	Journalisation des appels d'API Amazon Rekognition à l'aide de AWS CloudTrail	06/04/2018
Amazon Route 53	Utilisation de AWS CloudTrail pour capturer des demandes envoyées à l'API Route 53	11/02/2015

AWS Service	CloudTrail Sujets	Début de la prise en charge
Contrôleur de récupération des applications Amazon Route 53	Journalisation des appels d'API Amazon Route 53 Application Recovery Controller à l'aide de AWS CloudTrail	27/07/2021
Amazon S3	Journalisation des appels d'API Amazon S3 en utilisant AWS CloudTrail	Événements de gestion : 01/09/2015 Événements de données : 21/11/2016
Amazon S3 Glacier	Journalisation des appels d'API S3 Glacier en utilisant AWS CloudTrail	11/12/2014
Amazon SageMaker	Journalisation des appels SageMaker d'API Amazon avec AWS CloudTrail	11/01/2018
Amazon Security Lake	Journalisation des appels d'API Amazon Security Lake à l'aide de CloudTrail	30/05/2023
Amazon Simple Email Service (Amazon SES)	Journalisation des appels d'API Amazon SES en utilisant AWS CloudTrail	07/05/2015
Amazon Simple Notification Service (Amazon SNS)	Journalisation des appels d'API Amazon SNS à l'aide de AWS CloudTrail	09/10/2014
Amazon Simple Queue Service (Amazon SQS)	Journalisation des actions de l'API Amazon SQS à l'aide de AWS CloudTrail	16/07/2014

AWS Service	CloudTrail Sujets	Début de la prise en charge
Amazon Simple Workflow Service (Amazon SWF)	Enregistrement des appels d'API avec AWS CloudTrail	Événements de gestion : 13/05/2014 Données relatives aux événements : 14/02/2024
Amazon Textract	Journalisation des appels d'API Amazon Textract avec AWS CloudTrail	05/29/2019
Amazon Timestream	Enregistrement des appels d'API Timestream avec AWS CloudTrail	30/09/2020
Amazon Transcribe	Enregistrement des appels d'API Amazon Transcribe avec AWS CloudTrail	28/06/2018
Amazon Translate	Journalisation des appels d'API Amazon Translate à l'aide d' AWS CloudTrail	04/04/2018
Amazon Verified Permissions	Journalisation des appels d'API Amazon Verified Permissions à l'aide de AWS CloudTrail	13/06/2023
Amazon Virtual Private Cloud (Amazon VPC)	Journalisation des appels d'API à l'aide AWS CloudTrail L'API Amazon VPC est un sous-ensemble de l'API Amazon EC2.	13/11/2013
Amazon VPC Lattice	CloudTrail journaux	31 MARS 2023

AWS Service	CloudTrail Sujets	Début de la prise en charge
Analyseur d'accessibilité Amazon VPC	Journalisation des appels d'API Reachability Analyzer à l'aide de AWS CloudTrail	27/11/2023
Amazon WorkDocs	Journalisation des appels WorkDocs d'API Amazon en utilisant AWS CloudTrail	27/08/2014
Amazon WorkMail	Journalisation des appels WorkMail d'API Amazon à l'aide AWS CloudTrail	12/12/2017
Amazon WorkSpaces	Journalisation des appels WorkSpaces d'API Amazon en utilisant CloudTrail	09/04/2015
Amazon WorkSpaces Thin Client	Journalisation des appels d'API Amazon WorkSpaces Thin Client à l'aide de AWS CloudTrail	26/11/2023
WorkSpaces Site Web d'Amazon	Journalisation des appels d'API WorkSpaces Web Amazon à l'aide de AWS CloudTrail	30/11/2021
Application Auto Scaling	Journalisation des appels d'API Application Auto Scaling avec AWS CloudTrail	31/10/2016
AWS Amplify	Journalisation des appels d'API Amplify à l'aide de AWS CloudTrail	30/11/2020

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS App Mesh	Journalisation des appels d'API App Mesh à l'aide de AWS CloudTrail	AWS App Mesh 30/10/2019 Service de gestion App Mesh Envoy 18/03/2022
AWS App Runner	Journalisation des appels d'API App Runner avec AWS CloudTrail	18/05/2021
AWS AppConfig	Enregistrement des appels AWS AppConfig d'API à l'aide de AWS CloudTrail	Événements de gestion : 31/07/2020 Données relatives aux événements : 01/04/2024
AWS AppFabric	Journalisation des appels AWS AppFabric d'API à l'aide AWS CloudTrail	27/06/2023
AWS Profileur des coûts d'application	AWS Référence de l'API Application Cost Profiler	13/05/2021
AWS Application Discovery Service	Journalisation des appels d'API Application Discovery Service à l'aide de AWS CloudTrail	12/05/2016
AWS Service de transformation des applications	(Service principal utilisé par AWS des outils tels que AWS Microservice Extractor pour .NET)	26/08/2023
AWS AppSync	Journalisation des appels d' AWS AppSync API avec AWS CloudTrail	13/02/2018

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Artifact	Journalisation des appels d' AWS Artifact API avec AWS CloudTrail	27/01/2023
AWS Audit Manager	Journalisation des appels d' AWS Audit Manager API avec AWS CloudTrail	07/12/2020
AWS Auto Scaling	Journalisation des appels d' AWS Auto Scaling API en utilisant CloudTrail	15/08/2018
AWS Échange de données B2B	Enregistrement des appels d'API d'échange de données AWS B2B à l'aide de AWS CloudTrail	01/12/2023
AWS Backup	Journalisation des appels d' AWS Backup API avec AWS CloudTrail	04/02/2019
AWS Batch	Journalisation des appels d' AWS Batch API avec AWS CloudTrail	10/01/2018
AWS Billing and Cost Management	Journalisation des appels d' AWS Billing and Cost Management API avec AWS CloudTrail	07/06/2018
AWS Billing Conductor	Enregistrement des appels AWS Billing Conductor d'API à l'aide de AWS CloudTrail	03/12/2024
AWS BugBust	Enregistrement des appels BugBust d'API à l'aide de CloudTrail	24/06/2021

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Certificate Manager	Utilisation de AWS CloudTrail	25/03/2016
AWS Clean Rooms	Enregistrement des appels AWS Clean Rooms d'API à l'aide de AWS CloudTrail	21/03/2023
AWS Cloud Map	Journalisation des appels d' AWS Cloud Map API avec AWS CloudTrail	11-28-2018
AWS Cloud9	Journalisation des appels d' AWS Cloud9 API avec AWS CloudTrail	21/01/2019
AWS CloudFormation	Enregistrement des appels d' AWS CloudFormation API AWS CloudTrail	02/04/2014
AWS CloudHSM	Journalisation des appels d' AWS CloudHSM API en utilisant AWS CloudTrail	08/01/2015
AWS CloudShell	Connexion et surveillance AWS CloudShell	15 décembre 2020
AWS CloudTrail	AWS CloudTrail Référence d'API (tous les appels d' CloudTrail API sont enregistr és par CloudTrail.)	13/11/2013
AWS CodeArtifact	Journalisation des appels d' CodeArtifact API avec AWS CloudTrail	10/06/2020
AWS CodeBuild	Journalisation des appels d' AWS CodeBuild API avec AWS CloudTrail	01/12/2016

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS CodeCommit	Journalisation des appels d' AWS CodeCommit API avec AWS CloudTrail	11/01/2017
AWS CodeDeploy	Surveillance des déploiements avec AWS CloudTrail	16/12/2014
AWS CodePipeline	Journalisation des appels d' CodePipeline API avec AWS CloudTrail	09/07/2015
AWS CodeStar	Journalisation des appels d' AWS CodeStar API avec AWS CloudTrail	14/06/2017
AWS CodeStar Notifications	Journalisation AWS CodeStar des appels d'API de notifications avec AWS CloudTrail	11/05/2019
AWS Config	Enregistrement des appels AWS Config d'API par with AWS CloudTrail	10/02/2015
AWS Catalogue de contrôle	Journalisation AWS des appels d'API Control Catalog à l'aide de AWS CloudTrail	08/04/2024
AWS Control Tower	AWS Control Tower Actions de journalisation avec AWS CloudTrail	12/08/2019
AWS Data Pipeline	Journalisation des appels d' AWS Data Pipeline API en utilisant AWS CloudTrail	02/12/2014

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Database Migration Service (AWS DMS)	Enregistrement des appels AWS Database Migration Service d'API à l'aide de AWS CloudTrail	04/02/2016
AWS DataSync	Journalisation des appels d' AWS DataSync API avec AWS CloudTrail	11-26-2018
AWS Deadline Cloud	Enregistrement des appels avec CloudTrail	02/04/2024
AWS Device Farm	Journalisation des appels d' AWS Device Farm API en utilisant AWS CloudTrail	13/07/2015
AWS Direct Connect	Enregistrement des appels d' AWS Direct Connect API AWS CloudTrail	08/03/2014
AWS Directory Service	Journalisation des appels d' AWS Directory Service API en utilisant CloudTrail	14/05/2015
AWS Elastic Beanstalk (Elastic Beanstalk)	Utilisation des appels d'API Elastic Beanstalk avec AWS CloudTrail	31/03/2014
AWS Elastic Disaster Recovery	Enregistrement des appels AWS Elastic Disaster Recovery d'API à l'aide de AWS CloudTrail	17/11/2021
AWS Elemental MediaConnect	Journalisation des appels d' AWS Elemental MediaConnect API avec AWS CloudTrail	11-27-2018

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Elemental MediaConvert	Journalisation des appels d' AWS Elemental MediaConvert API avec CloudTrail	27/11/2017
AWS Elemental MediaLive	Journalisation des appels d' MediaLiveAPI avec AWS CloudTrail	19/01/2019
AWS Elemental MediaPackage	Journalisation des appels d' AWS Elemental MediaPackage API avec AWS CloudTrail	12-21-2018
AWS Elemental MediaStore	Journalisation des appels d' AWS Elemental MediaStore API avec CloudTrail	27/11/2017
AWS Elemental MediaTailor	Journalisation des appels d' AWS Elemental MediaTailor API avec AWS CloudTrail	02/11/2019
AWS Résolution de l'entité	Enregistrement des appels d'API de résolution d' AWS entités à l'aide de A AWS CloudTrail	26/07/2023
AWS Fault Injection Service	Enregistrez les appels d'API avec AWS CloudTrail	15/03/2021
AWS Firewall Manager	Journalisation des appels d' AWS Firewall Manager API avec AWS CloudTrail	05/04/2018
AWS Global Accelerator	Enregistrement des appels d'API AWS Global Accelerator avec AWS CloudTrail	11-26-2018

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Glue	AWS Glue Opérations de journalisation en utilisant AWS CloudTrail	07/11/2017
AWS Ground Station	Journalisation des appels d' AWS Ground Station API avec AWS CloudTrail	31/05/2019
AWS Health	Journalisation des appels d' AWS Health API avec AWS CloudTrail	21/11/2016
AWS Health Dashboard	Journalisation des appels d' AWS Health API avec AWS CloudTrail	01/12/2016
AWS HealthImaging	Journalisation des appels AWS HealthImaging d'API à l'aide AWS CloudTrail	26/07/2023
AWS HealthLake	Journalisation des appels d' AWS HealthLake API avec AWS CloudTrail	07/12/2020
AWS HealthOmics	Journalisation des appels AWS HealthOmics d'API à l'aide AWS CloudTrail	29/11/2022
AWS IAM Identity Center	Journalisation des appels d'API IAM Identity Center avec AWS CloudTrail	07/12/2017
AWS Identity and Access Management (JE SUIS)	Journalisation des événement s IAM avec AWS CloudTrail	13/11/2013

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS IoT	Journalisation des appels d' AWS IoT API avec AWS CloudTrail	11/04/2016
AWS IoT 1-Click	Journalisation des appels d' AWS IoT 1-Click API avec AWS CloudTrail	14/05/2018
AWS IoT Analytique	Journalisation AWS IoT des appels d'API Analytics avec AWS CloudTrail	23/04/2018
AWS IoT Événements	Journalisation AWS IoT des appels d'API des événements avec AWS CloudTrail	06/11/2019
AWS IoT Greengrass	Journalisation des appels d' AWS IoT Greengrass API avec AWS CloudTrail	10-29-2018
AWS IoT Greengrass V2	Enregistrez les appels d'API AWS IoT Greengrass V2 avec AWS CloudTrail	14/12/2020
AWS IoT SiteWise	Journalisation des appels d' AWS IoT SiteWise API avec AWS CloudTrail	04/29/2020
AWS Key Management Service (AWS KMS)	Enregistrement des appels AWS KMS d'API à l'aide de AWS CloudTrail	12/11/2014
AWS Lake Formation	Enregistrement des appels AWS Lake Formation d'API à l'aide de AWS CloudTrail	08/09/2019

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Lambda	Journalisation des appels d' AWS Lambda API en utilisant AWS CloudTrail	Événements de gestion : 09/04/2015 Événements de données : 30/11/2017
AWS Launch Wizard	Enregistrement des appels AWS Launch Wizard d'API à l'aide de AWS CloudTrail	08/11/2023
AWS License Manager	Journalisation des appels d'API AWS License Manager avec AWS CloudTrail	01/03/2019
AWS Mainframe Modernization	Enregistrement des appels AWS Mainframe Modernization d'API à l'aide de AWS CloudTrail	08/06/2022
AWS Managed Services	Gestion des journaux dans AMS Accelerate	21/12/2016
AWS Marketplace Accords	Contrats de journalisation des appels d'API en utilisant AWS CloudTrail	01/09/2023
AWS Marketplace Service de déploiement	Enregistrement des appels AWS Marketplace du service de déploiement avec CloudTrail	29/11/2023
AWS Marketplace Découverte	Journalisation des appels de l'API AWS Marketplace Discovery en utilisant AWS CloudTrail	15 décembre 2022

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Marketplace Service de comptage	Journalisation des appels d' AWS Marketplace API avec AWS CloudTrail	08/22/2018
AWS Migration Hub	Journalisation AWS des appels d'API du Migration Hub avec AWS CloudTrail	14/08/2017
AWS Network Firewall	Journalisation des appels à l' AWS Network Firewall API avec AWS CloudTrail	17/11/2020
AWS OpsWorks for Chef Automate	Journalisation des appels d' AWS OpsWorks for Chef Automate API avec AWS CloudTrail	16/07/2018
AWS OpsWorks for Puppet Enterprise	Journalisation OpsWorks des appels d'API Puppet Enterprise avec AWS CloudTrail	16/07/2018
AWS OpsWorks Stacks	Journalisation des appels d' AWS OpsWorks Stacks API avec AWS CloudTrail	04/06/2014
AWS Organizations	Journalisation des appels d' AWS Organizations API avec AWS CloudTrail	27/02/2017
AWS Outposts	Journalisation des appels d' AWS Outposts API avec AWS CloudTrail	04/02/2020
AWS Panorama	Référence d'API AWS Panorama	20/10/2021

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Payment Cryptography	Enregistrement des appels AWS Payment Cryptography d'API à l'aide de AWS CloudTrail	08/06/2023
AWS 5G privée	Enregistrement des appels AWS privés de l'API 5G à l'aide de AWS CloudTrail	08/11/2022
AWS Private Certificate Authority (AWS Private CA)	En utilisant CloudTrail	04/04/2018
AWS Proton	Connexion et surveillance AWS Proton	09/06/2021
AWS re:Post Privé	Journalisation des appels AWS re:Post d'API privés à l'aide de AWS CloudTrail	26/11/2023
AWS Resilience Hub	AWS CloudTrail	10/11/2021
AWS Resource Access Manager (AWS RAM)	Journalisation des appels d' AWS RAM API avec AWS CloudTrail	11-20-2018
Explorateur de ressources AWS	Enregistrement des appels Explorateur de ressources AWS d'API à l'aide de AWS CloudTrail	07/11/2022
AWS Resource Groups	Journalisation et surveillance dans Resource Groups	29/06/2018
AWS RoboMaker	Journalisation des appels d' AWS RoboMaker API avec AWS CloudTrail	16/01/2019

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Secrets Manager	Surveillez l'utilisation de vos AWS Secrets Manager secrets	05/04/2018
AWS Security Hub	Journalisation des appels d' AWS Security Hub API avec AWS CloudTrail	11-27-2018
AWS Security Token Service (AWS STS)	Journalisation des événement s IAM avec AWS CloudTrail La rubrique IAM inclut des informations pour AWS STS.	13/11/2013
AWS Serverless Application Repository	Journalisation des appels d' AWS Serverless Application Repository API avec AWS CloudTrail	20/02/2018
AWS Service Catalog	Journalisation des appels d'API Service Catalog avec AWS CloudTrail	06/07/2016
AWS Shield	Les appels d'API avancés de Logging Shield avec AWS CloudTrail	08/02/2018
AWS Snowball Bord	Journalisation des appels d'API AWS Snowball Edge avec AWS CloudTrail	25/01/2019
AWS Step Functions	Journalisation des appels d' AWS Step Functions API avec AWS CloudTrail	01/12/2016
AWS Storage Gateway	Journalisation des appels d'API Storage Gateway en utilisant AWS CloudTrail	16/12/2014

AWS Service	CloudTrail Sujets	Début de la prise en charge
AWS Support	Journalisation des appels d' AWS Support API avec AWS CloudTrail	21/04/2016
AWS Support Recommandations (aperçu)	Journalisation AWS Support des appels d'API de recommandations avec AWS CloudTrail	22/05/2024
AWS Systems Manager	Journalisation des appels d' AWS Systems Manager API avec AWS CloudTrail	29/11/2017
AWS Systems Manager Incident Manager	Enregistrement des appels d'API AWS Systems Manager Incident Manager à l'aide de AWS CloudTrail	10/05/2021
AWS Générateur de réseaux de télécommunications (AWS TNB)	Enregistrement des appels d'API AWS Telco Network Builder à l'aide de AWS CloudTrail	21/02/2023
AWS Transfer for SFTP	Journalisation des appels d' AWS Transfer for SFTP API avec AWS CloudTrail	08/01/2019
AWS Transit Gateway	Journalisation des appels d'API pour votre Transit Gateway à l'aide de AWS CloudTrail	11-26-2018
AWS Trusted Advisor	Journalisation des actions de AWS Trusted Advisor la console avec AWS CloudTrail	22/10/2020

AWS Service	CloudTrail Sujets	Début de la prise en charge
Accès vérifié par AWS	Enregistrez les appels Accès vérifié par AWS d'API à l'aide de AWS CloudTrail	27/04/2023
AWS WAF	Journalisation des appels d' AWS WAF API avec AWS CloudTrail	28/04/2016
AWS Well-Architected Tool	Journalisation des appels d' AWS Well-Architected Tool API avec AWS CloudTrail	15 décembre 2020
AWS X-Ray	Journalisation des appels d' AWS X-Ray API avec CloudTrail	25/04/2018
Elastic Load Balancing	AWS CloudTrail Journalisation pour votre Classic Load Balancer et AWS CloudTrail journalisation pour votre Application Load Balancer	04/04/2014
Mises à jour OTA (par voie hertzienne) de FreeRTOS	Enregistrement des appels d'API AWS IoT OTA avec AWS CloudTrail	05/22/2019
Service Quotas	Journalisation des appels d'API Service Quotas à l'aide de AWS CloudTrail	24/06/2019

CloudTrail services non pris en charge

Les services qui sont encore en version préliminaire, qui ne sont pas encore disponibles pour une mise à disposition générale (GA) ou qui ne disposent pas d'API publiques ne sont pas considérés comme pris en charge.

En outre, les AWS services et événements suivants ne sont pas pris en charge :

- AWS Import/Export
- Événements spécifiques à la politique de point de terminaison Amazon VPC

Pour obtenir la liste des AWS services pris en charge, consultezAWS sujets de service pour CloudTrail.

Quotas dans AWS CloudTrail

Le tableau suivant décrit les quotas (anciennement appelés limites) au sein de CloudTrail. CloudTrail n'a pas de quotas ajustables. Pour plus d'informations sur les autres quotas dans AWS, consultez la section Quotas AWS de service.

Ressource	Quota par défaut	Commentaires
Journaux de suivi par région	5	Ce quota ne peut pas être augmenté.
API Get, Describe et List	10 transactions par seconde (TPS)	Le nombre maximum de demandes d'opérations par seconde sans être limité. Les `StartQuery` API `CancelQuery` `LookupEvents` ,`ListInsightsMetricData` ,`PutAuditEvents` , et ne sont pas incluses dans cette catégorie.
CancelQuery, StartQuery API	3 transactions par seconde (TPS)	Le nombre maximum de demandes d'opérations par seconde sans être limité. Ce quota ne peut pas être augmenté.

Ressource	Quota par défaut	Commentaires
LookupEvents API	2 transactions par seconde (TPS)	Le nombre maximum de demandes d'opérations par seconde sans être limité. Ce quota ne peut pas être augmenté.
ListInsightsMetricData API	1 transaction par seconde (TPS)	Le nombre maximum de demandes d'opérations par seconde sans être limité. Ce quota ne peut pas être augmenté.
PutAuditEvents API	100 transactions par seconde (TPS)	Le nombre maximum de demandes d'opérations par seconde sans être limité. Ce quota ne peut pas être augmenté.
Toutes les autres API	1 transaction par seconde (TPS)	Le nombre maximum de demandes d'opérations par seconde sans être limité. Ce quota ne peut pas être augmenté.

Ressource	Quota par défaut	Commentaires
Entrepôts de données d'événement	10	Le nombre maximum d'entrepôts de données d'événement dont vous pouvez disposer dans chaque Région AWS. Cela inclut les entrepôts de données d'événement à région unique pour la région ainsi que tous les entrepôts de données d'événement multi-régions pour toutes les Régions AWS. Cela inclut les entrepôts de données d'événement à toutes les étapes du cycle de vie. Ce quota ne peut pas être augmenté.
Canaux	25	Ce quota s'applique aux canaux utilisés pour les intégrations de CloudTrai l Lake avec des sources d'événements extérieures AWS, et ne s'applique pas aux canaux liés aux services. Ce quota ne peut pas être augmenté.

Ressource	Quota par défaut	Commentaires
Requêtes simultanées	10	Le nombre maximum de requêtes en file d'attente ou en cours d'exécution que vous pouvez exécuter simultané ment dans CloudTrail Lake. Ce quota ne peut pas être augmenté.
Événements par PutAuditE vents demande	100	Vous pouvez ajouter jusqu'à 100 événements d'activité (ou jusqu'à 1 Mo) par demande `PutAuditEvents` . Ce quota ne peut pas être augmenté.
Sélecteurs d'événements	5 par journal de suivi	Ce quota ne peut pas être augmenté.

Ressource	Quota par défaut	Commentaires
Sélecteurs d'événements avancés	500 conditions sur tous les sélecteurs d'événements avancés	Si un journal de suivi ou un stockage de données d'événement utilise des sélecteurs d'événements avancés, un maximum de 500 valeurs totales est autorisé pour l'ensemble des conditions dans tous les sélecteurs d'événements avancés. À moins qu'un journal de suivi ou un stockage de données d'événement journalise les événements de données sur l'ensemble des ressources, notamment tous les compartiments S3 ou toutes les fonctions Lambda, la limite est fixée à 250 ressources de données. Les ressources de données peuvent être réparties sur les sélecteurs d'événements, mais le total ne peut excéder 250. Ce quota ne peut pas être augmenté.

Ressource	Quota par défaut	Commentaires
Ressources de données dans les sélecteurs d'événements	250 sur l'ensemble des sélecteurs d'événements d'un journal de suivi	Si vous choisissez de limiter les événements de données à l'aide de sélecteurs d'événements ou de sélecteurs d'événements avancés, le nombre total de ressources de données ne peut excéder 250 sur l'ensemble des sélecteurs d'événements d'un journal de suivi. Le nombre de ressources maximal pour un sélecteur d'événements est configurable jusqu'à 250. Cette limite supérieure est autorisée uniquement si le nombre total de ressources de données ne dépasse pas 250 sur l'ensemble des sélecteurs d'événements. Exemples : • Un journal de suivi avec 5 sélecteurs d'événements, chacun configuré avec 50 ressources de données, est autorisé. (5*50=250) • Un journal de suivi avec 5 sélecteurs d'événements, dont 3 sont configurés avec 50 ressources de données, 1 avec 99 ressources de données et 1 avec 1 ressource de données,

Ressource	Quota par défaut	Commentaires
		est également autorisé. ((3*50)+1+99=250) • Un journal de suivi avec 5 sélecteurs d'événements, dont tous sont configuré s avec 100 ressources de données, n'est pas autorisé. (5*100=500) Les sélecteurs d'événeme nts s'appliquent uniquemen t aux journaux de suivi. Pour les stockages de données d'événement, vous devez utiliser des sélecteurs d'événements avancés. Ce quota ne peut pas être augmenté. Le quota ne s'applique pas si vous choisissez de journaliser les événements de données sur toutes les ressources, notamment tous les compartim ents S3 ou toutes les fonctions Lambda.

Ressource	Quota par défaut	Commentaires
Taille de l'événement	Toutes les versions d'événements : les événements de plus de 256 Ko ne peuvent pas être envoyés à CloudWatch Logs Version de l'événement 1.05 et plus récente : limite de taille totale de l'événement de 256 Ko	Amazon CloudWatch Logs et Amazon autorisent EventBridge chacun une taille d'événement maximale de 256 Ko. CloudTrail n'envoie pas d'événements de plus de 256 Ko à CloudWatch Logs ou EventBridge. À partir de la version 1.05 de l'événement, les événements ont une taille maximale de 256 Ko. Cela permet d'empêcher l'exploitation par des acteurs malveillants et de permettre à d'autres AWS services, tels que CloudWatch Logs et EventBridge.
CloudTrail taille du fichier envoyé à Amazon S3	Fichier ZIP équivalant à 50 Mo, après compression	Pour les événements de gestion et de données, CloudTrail envoie les événements à S3 dans des fichiers ZIP (compressés) de 50 Mo maximum. Si cette option est activée en cours, les notifications de livraison des journaux sont envoyées par Amazon SNS après l' CloudTrail envoi de fichiers ZIP à S3.

Commencer à utiliser les AWS CloudTrail didacticiels

Si vous êtes nouveau dans ce AWS CloudTrail domaine, ces didacticiels peuvent vous aider à apprendre à utiliser ses fonctionnalités.

Rubriques

Accorder des autorisations d'utilisation CloudTrail

Pour créer, mettre à jour et gérer CloudTrail des ressources telles que les parcours, les magasins de données d'événements et les canaux, vous devez accorder des autorisations d'utilisation CloudTrail. Cette section fournit des informations sur les politiques gérées disponibles pour CloudTrail.

> **Note**
>
> Les autorisations que vous accordez aux utilisateurs pour effectuer des tâches d' CloudTrail administration ne sont pas les mêmes que CloudTrail celles requises pour envoyer des fichiers journaux dans des compartiments Amazon S3 ou envoyer des notifications aux rubriques Amazon SNS. Pour plus d'informations sur ces autorisations, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.
>
> Si vous configurez l'intégration avec Amazon CloudWatch Logs, cela nécessite CloudTrail également un rôle que celui-ci peut assumer pour transmettre des événements à un groupe de CloudWatch journaux Amazon Logs. Vous devez créer le rôle qui CloudTrail utilise. Pour plus d'informations, consultez Octroi de l'autorisation d'afficher et de configurer CloudWatch les informations Amazon Logs sur la CloudTrail console et Envoyer des événements à CloudWatch Logs.

Les politiques AWS gérées suivantes sont disponibles pour CloudTrail :

- AWSCloudTrail_FullAccess— Cette politique fournit un accès complet aux CloudTrail actions sur les CloudTrail ressources, telles que les sentiers, les magasins de données sur les événements et les canaux. Cette politique fournit les autorisations requises pour créer, mettre à jour et supprimer des CloudTrail traces, des banques de données d'événements et des chaînes.

  Cette politique fournit également des autorisations pour gérer le compartiment Amazon S3, le groupe de CloudWatch journaux pour les journaux et une rubrique Amazon SNS pour un suivi. Cependant, la politique `AWSCloudTrail_FullAccess` gérée n'autorise pas la suppression du compartiment Amazon S3, du groupe de CloudWatch journaux pour les journaux ou d'une rubrique Amazon SNS. Pour plus d'informations sur les politiques gérées pour d'autres AWS services, consultez le Guide de référence des politiques AWS gérées.

  > **Note**
  >
  > La AWSCloudTrail_FullAccesspolitique n'est pas destinée à être largement partagée entre vous Compte AWS. Les utilisateurs ayant ce rôle peuvent désactiver ou reconfigurer les fonctions d'audit les plus sensibles et les plus importantes dans leur Comptes AWS. Pour cette raison, vous ne devez appliquer cette politique qu'aux administrateurs de compte. Vous devez contrôler et surveiller étroitement l'utilisation de cette politique.

- AWSCloudTrail_ReadOnlyAccess— Cette politique accorde des autorisations pour consulter la CloudTrail console, y compris les événements récents et l'historique des événements. Cette politique vous permet également de consulter les journaux de suivi, les entrepôts de données d'événement et les canaux existants. Les rôles et les utilisateurs soumis à cette politique peuvent télécharger l'historique des événements, mais ils ne peuvent pas créer ou mettre à jour des journaux de suivi, des entrepôts de données d'événement ou des canaux.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.

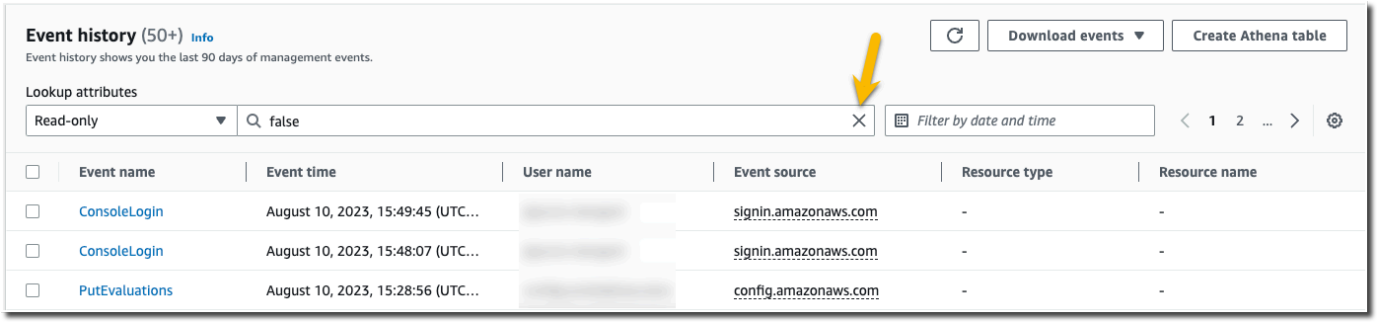
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Afficher l'historique des événements

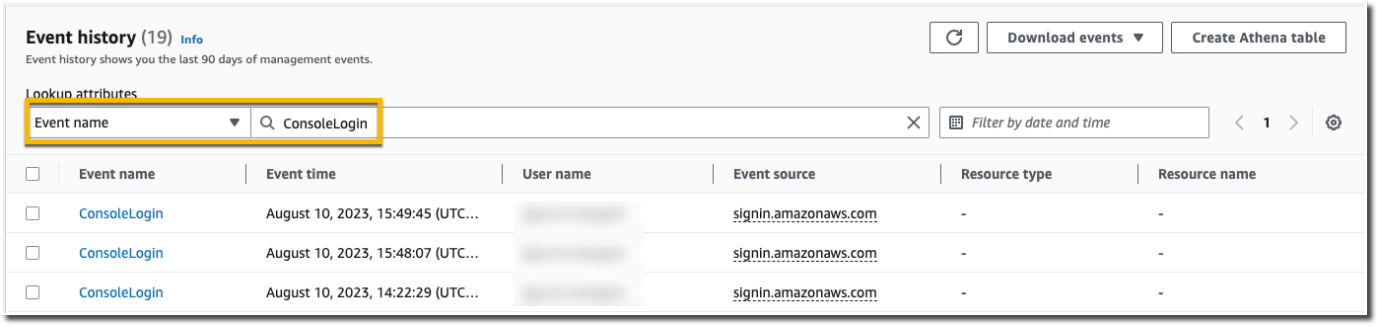
Cette section décrit comment utiliser la page Historique des CloudTrail événements de la CloudTrail console pour afficher les 90 derniers jours d'événements de gestion pour vous Compte AWS pour le moment Région AWS.

Pour consulter l'historique des événements

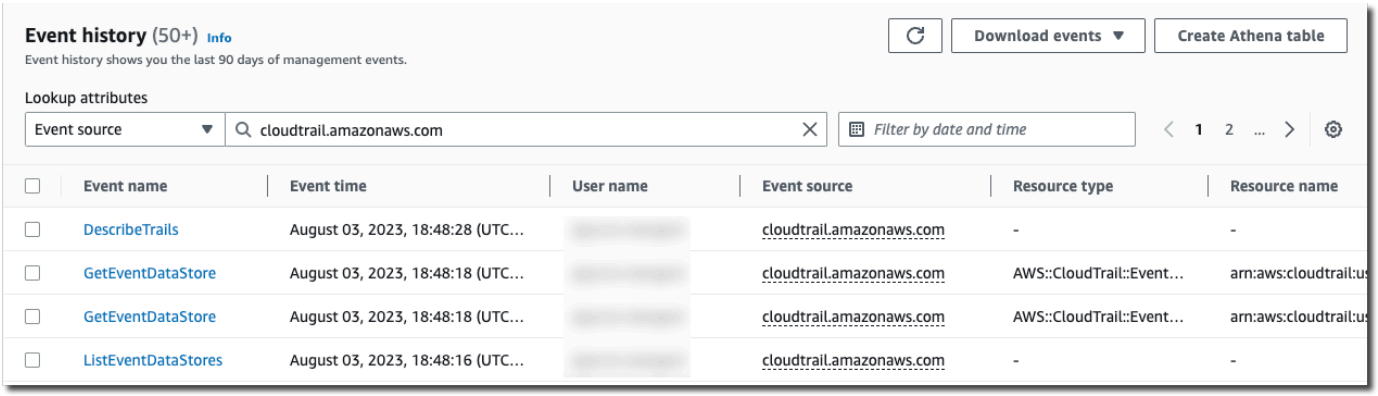
1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, choisissez Event history (Historique des événements). Vous voyez une liste filtrée des événements, avec les événements les plus récents affichés d'abord. Le filtre par défaut pour les événements est Lecture seule, défini sur false. Il est possible d'effacer ce filtre en choisissant X à droite du filtre. Vous pouvez effectuer des recherches d'événement dans l'Historique des événements en filtrant les événements sur un seul attribut.



3. Choisissez un attribut à filtrer et entrez la valeur complète de l'attribut. CloudTrail Impossible de filtrer sur une valeur partielle. Par exemple, pour afficher tous les événements de connexion à la console, choisissez le filtre Nom d'événement et spécifiez ConsoleLoginla valeur de l'attribut.



Ou, pour consulter les événements CloudTrail de gestion récents, choisissez Source de l'événement et spécifiez`cloudtrail.amazonaws.com`.



4. Pour consulter un événement de gestion spécifique, choisissez le nom de l'événement. Sur la page des détails de l'événement, vous pouvez consulter les détails de l'événement, les ressources référencées et l'enregistrement de l'événement.
5. Pour comparer des événements, sélectionnez jusqu'à cinq événements en remplissant leurs cases à cocher dans la marge gauche de la table Historique des événements. Vous pouvez consulter les détails des événements sélectionnés side-by-side dans le tableau Comparer les détails des événements.
6. Vous pouvez enregistrer l'historique des événements en le téléchargeant en tant que fichier au format JSON ou CSV. Le téléchargement de l'historique de votre événement peut prendre quelques minutes.

Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.

Créez une trace pour consigner les événements de gestion

Pour votre premier parcours, nous vous recommandons de créer un parcours qui enregistre tous les événements de gestion dans toutes les AWS régions et qui n'enregistre aucun événement lié aux données. Des exemples d'événements de gestion incluent des événements liés à la sécurité, tels que les événements IAM `CreateUser` et `AttachRolePolicy`, les événements de ressource tels que `RunInstances` et `CreateBucket`, et bien plus encore. Vous allez créer un compartiment Amazon S3 dans lequel vous stockerez les fichiers journaux du journal dans le cadre de la création du journal dans la CloudTrail console.

> **Note**
>
> Ce didacticiel suppose que vous créez votre premier journal de suivi. En fonction du nombre de sentiers que vous avez sur votre AWS compte et de la façon dont ces sentiers sont configurés, la procédure suivante peut entraîner des frais ou non. CloudTrail stocke les fichiers journaux dans un compartiment Amazon S3, ce qui entraîne des coûts. Pour plus d'informations sur la tarification, consultez Tarification AWS CloudTrail et Tarification Amazon S3.

Pour créer un journal de suivi

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le sélecteur de région, choisissez la AWS région dans laquelle vous souhaitez créer votre parcours. Il s'agit de la région d'origine pour le journal de suivi.

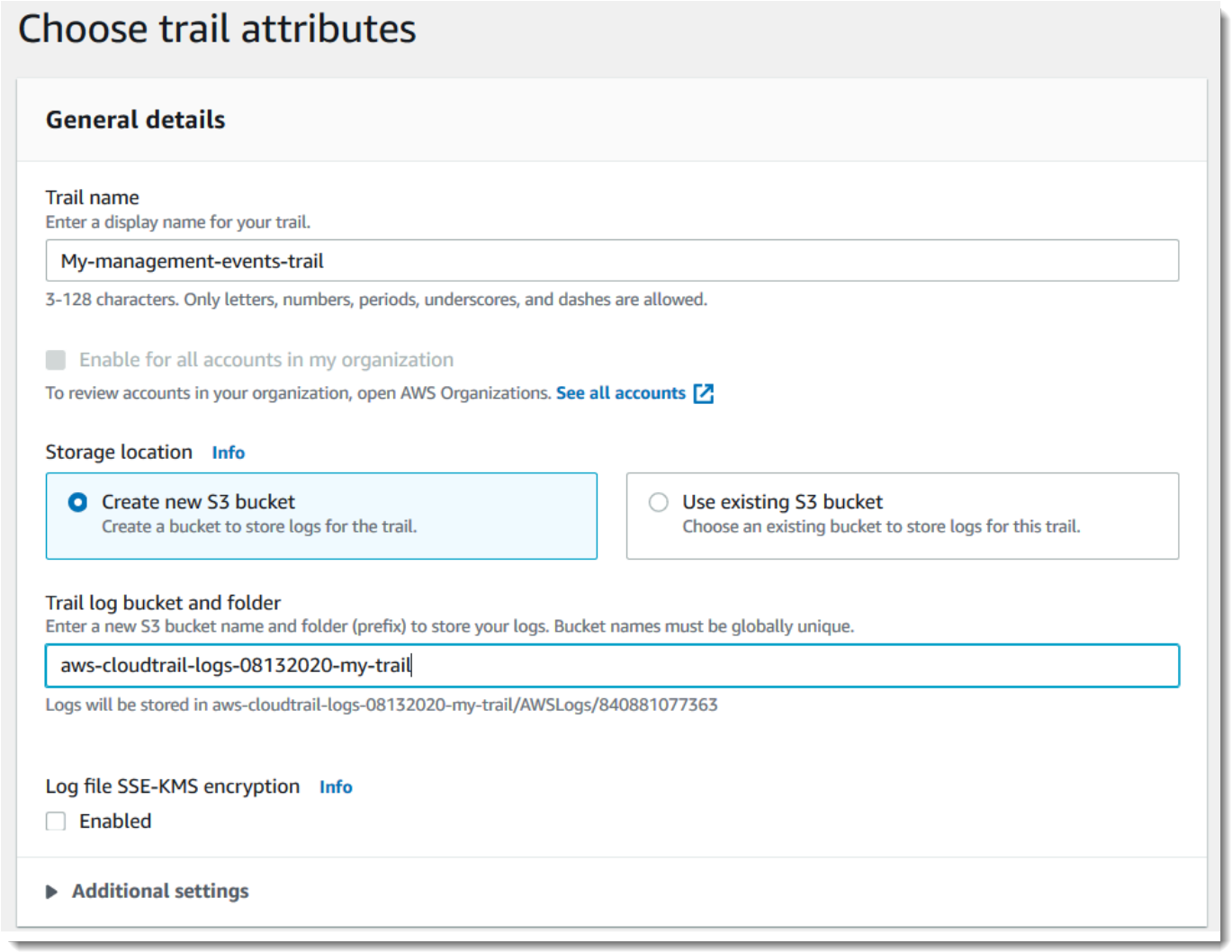
   > **Note**
   >
   > La région d'origine est la seule AWS région où vous pouvez consulter et mettre à jour le parcours une fois celui-ci créé, même s'il enregistre des événements dans toutes les AWS régions.

3. Sur la page d'accueil du CloudTrail service, sur la page des sentiers ou dans la section des sentiers de la page du tableau de bord, choisissez Créer un parcours.

4. Dans Trail name (Nom du journal de suivi), attribuez un nom à votre journal de suivi, par exemple *My-Management-Events-Trail*. Comme bonne pratique, utilisez un nom qui identifie rapidement l'objectif du journal de suivi. Dans ce cas, vous créez un journal de suivi qui journalise des événements de gestion.
5. Conservez le paramètre par défaut pour Activer pour tous les comptes de mon organisation. Cette option ne pourra pas être modifiée à moins que vous ayez des comptes configurés dans Organizations.
6. Sous Storage location (Emplacement de stockage), choisissez Create new S3 bucket (Créer un nouveau compartiment S3) pour créer un compartiment. Lorsque vous créez un bucket, il CloudTrail crée et applique les politiques de bucket requises. Si vous choisissez de créer un nouveau compartiment S3, votre politique IAM doit inclure une autorisation pour l'`s3:PutEncryptionConfiguration`action, car le chiffrement côté serveur est activé par défaut pour le compartiment. Donnez à votre bucket un nom qui le rende facilement identifiable.

   Pour retrouver plus facilement vos journaux, créez un nouveau dossier (également appelé préfixe) dans un compartiment existant pour stocker vos CloudTrail journaux.

   > **Note**
   >
   > Le nom de votre compartiment Amazon S3 doit être unique globalement. Pour plus d'informations, veuillez consulter la section Règles de dénomination de compartiment dans le Guide de l'utilisateur Amazon Simple Storage Service.



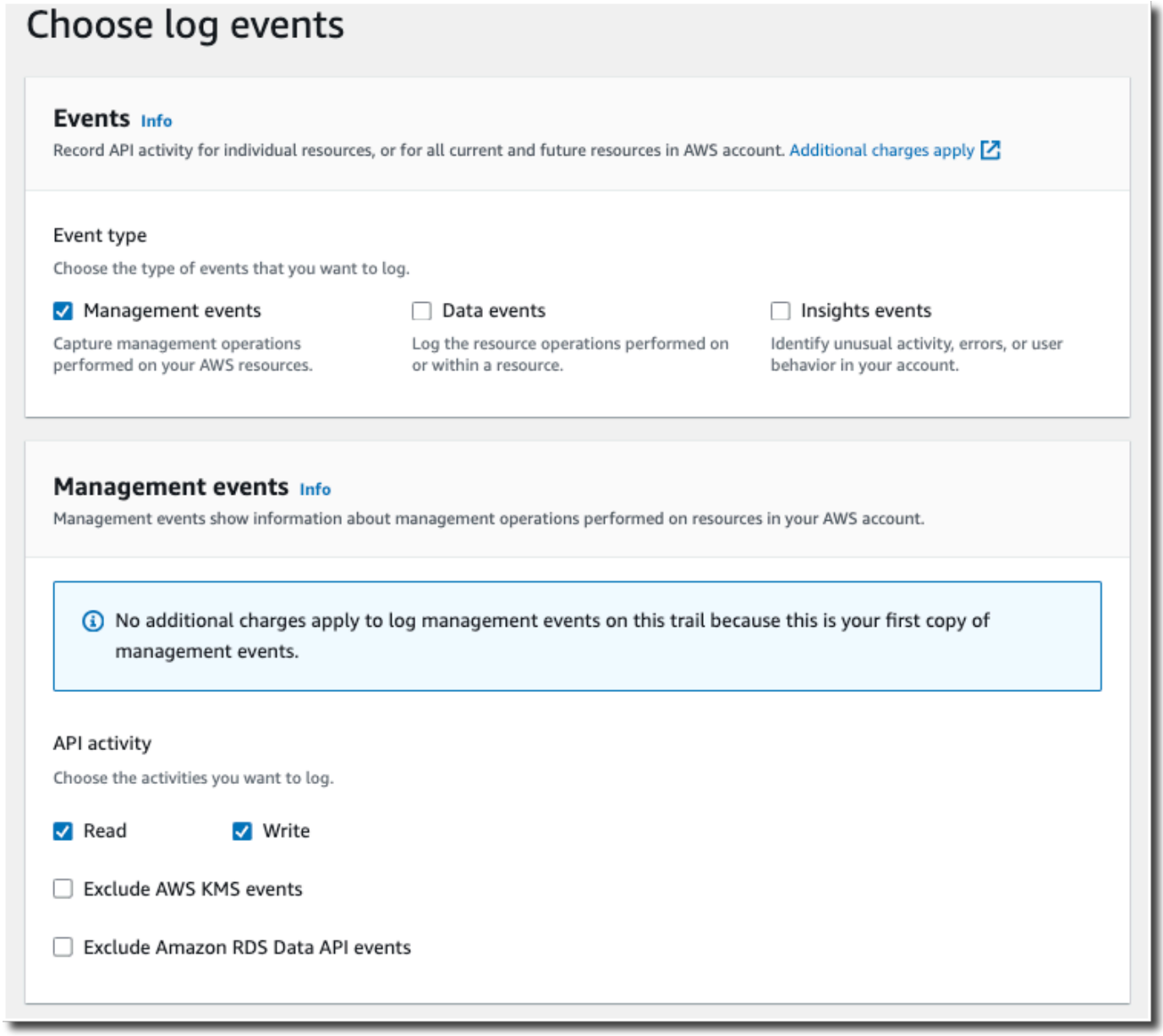
7. Supprimez la case à cocher pour désactiver le Chiffrement du fichier journal SSE-KMS. Par défaut, vos fichiers journaux sont chiffrés avec le chiffrement SSE de S3. Pour plus d'informations sur ce paramètre, consultez Utilisation du chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3).
8. Conserver les paramètres par défaut dans la section Additional settings (Paramètres supplémentaires).
9. Conservez les paramètres par défaut pour CloudWatch Logs. Pour le moment, n'envoyez pas de journaux à Amazon CloudWatch Logs.
10. Dans Balises, ajoutez une ou plusieurs identifications personnalisées (paires valeur-clé) à votre journal de suivi. Les balises peuvent vous aider à identifier vos CloudTrail traces et d'autres ressources, telles que les compartiments Amazon S3 qui contiennent des fichiers CloudTrail

journaux. Par exemple, il est possible d'attacher une balise portant le nom **`Compliance`** à la valeur **`Auditing`**.

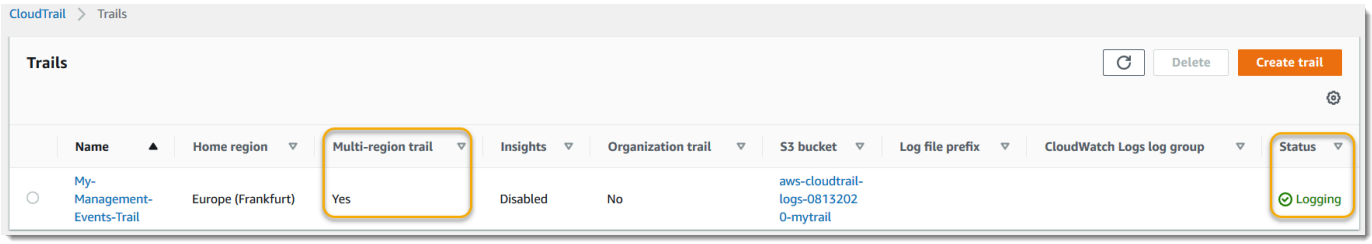
> **Note**
>
> Bien que vous puissiez ajouter des balises aux pistes lorsque vous les créez dans la CloudTrail console, et que vous puissiez créer un compartiment Amazon S3 pour stocker vos fichiers journaux dans la CloudTrail console, vous ne pouvez pas ajouter de balises au compartiment Amazon S3 depuis la CloudTrail console. Pour plus d'informations sur l'affichage et la modification des propriétés d'un compartiment Amazon S3, y compris l'ajout d'identifications à un compartiment, consultez le Guide de l'utilisateur Amazon S3.

Après la création des identifications, choisissez Suivant.

11. Dans la page Choisir des événements du journal, sélectionnez les types d'événements à journaliser. Pour ce journal de suivi, conservez par défaut les Événements de gestion. Dans la zone Événements de gestion, choisissez de journaliser les deux événements Lecture et Écriture, s'ils ne sont pas déjà sélectionnés. Laissez les cases à cocher Exclure les AWS KMS événements et Exclure les événements de l'API de données Amazon RDS vides pour consigner tous les événements de gestion.



12. Conserver les paramètres par défaut pour Événements de données et Événements Insights. Ce parcours n'enregistrera aucune donnée ni aucun événement CloudTrail Insights. Choisissez Next (Suivant).
13. Dans la page Vérifier et créer, vérifiez les paramètres que vous avez choisis pour votre journal de suivi. Choisissez Modifier pour retourner à la section souhaitée et y apporter les modifications nécessaires. Lorsque vous êtes prêt à créer votre journal de suivi, choisissez Créer un journal de suivi.
14. La page Journaux de suivi affiche votre nouveau journal fraîchement créé dans le tableau. Remarquez que le journal de suivi est défini en tant que Journal de suivi multi-régions par défaut, et cette journalisation est activée pour le journal de suivi par défaut.



Afficher les fichiers journaux

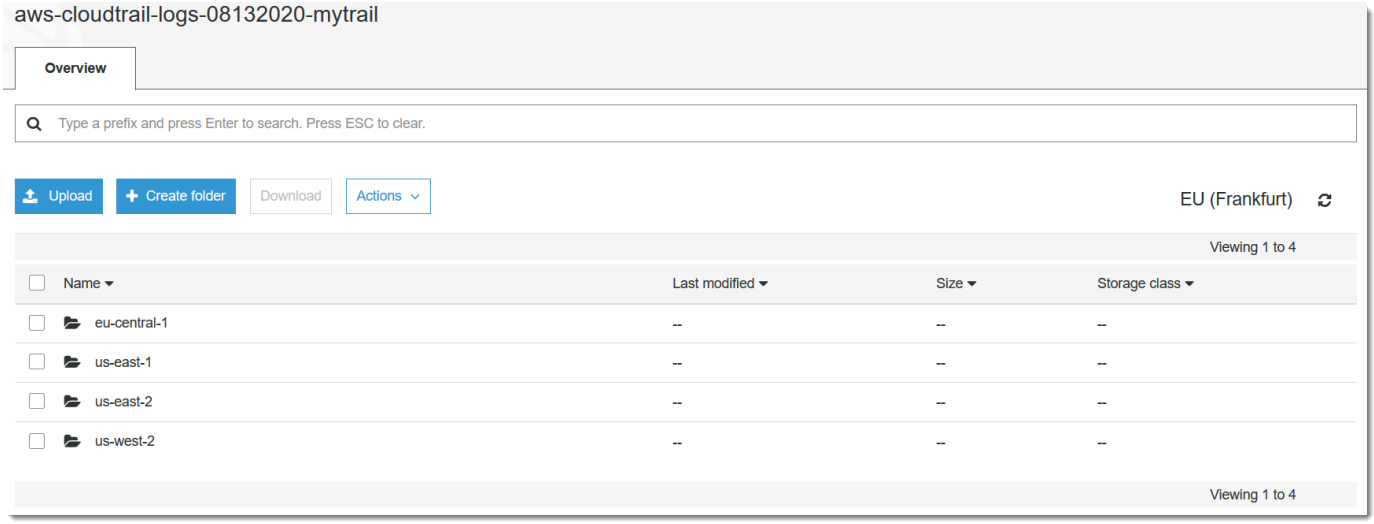
Environ 5 minutes en moyenne après la création de votre premier parcours, CloudTrail envoie le premier ensemble de fichiers journaux au compartiment Amazon S3 correspondant à votre parcours. Vous pouvez examiner ces fichiers et en savoir plus sur les informations qu'ils contiennent.

> **Note**
>
> CloudTrail fournit généralement des journaux dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti. Pour plus d'informations, consultez le Contrat de niveau de service (SLA)AWS CloudTrail.
> Si vous configurez mal votre trace (par exemple, si le compartiment S3 est inaccessible), vous CloudTrail tenterez de remettre les fichiers journaux à votre compartiment S3 pendant 30 jours, et ces attempted-to-deliver événements seront soumis aux frais standard. CloudTrail Pour éviter des frais sur un journal de suivi mal configuré, vous devez supprimer le journal de suivi.

Pour afficher les fichiers journaux

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, choisissez Journaux de suivi. Sur la page Journaux de suivi, recherchez le nom du journal de suivi que vous venez de créer (dans l'exemple, *`My-Management-Events-Trail`*).
3. Dans la ligne correspondant au parcours, choisissez la valeur du compartiment S3 (dans l'exemple, *`aws-cloudtrail-logs-08132020-mytrail`*).
4. La console Amazon S3 s'ouvre et affiche ce compartiment, dans la partie supérieure réservée aux fichiers journaux. Comme vous avez créé un journal qui enregistre les événements dans toutes les AWS régions, l'affichage s'ouvre au niveau qui indique le dossier de chaque région.

La hiérarchie de la navigation dans les compartiments Amazon S3 à ce niveau est bucket-name/AWS Logs/ account-id/. CloudTrail Choisissez le dossier de la AWS région dans laquelle vous souhaitez consulter les fichiers journaux. Par exemple, si vous souhaitez vérifier les fichiers journaux de la région USA Est (Ohio), choisissez us-east-2.



5. Accédez à la structure du dossier du compartiment de l'année, du mois et du jour pour lequel vous souhaitez consulter des journaux de suivi dans cette région. Pour ce jour, il existe un certain nombre de fichiers. Le nom des fichiers commence par votre identifiant de AWS compte et se termine par l'extension `.gz`. *Par exemple, si votre identifiant de compte est 123456789012, vous verrez des fichiers portant des noms similaires à celui-ci : 123456789012 _ _ us-east-2 _ 20190610t1255ABCDEExample .json.gz. CloudTrail*

   Pour afficher ces fichiers, vous pouvez les télécharger, les décompresser, puis les afficher dans un éditeur de texte brut ou un utilisateur de fichier JSON. Certains navigateurs prennent également en charge l'affichage .gz et les fichiers JSON directement. Nous vous recommandons d'utiliser un visualiseur JSON, car cela facilite l'analyse des informations contenues dans les fichiers CloudTrail journaux.

Planifier les prochaines étapes

Maintenant que vous avez un parcours, vous avez accès à un enregistrement permanent des événements et des activités sur votre AWS compte. Ce registre permanent vous aide également à répondre à vos besoins en termes de comptabilité et d'audit pour votre compte AWS . Cependant, vous pouvez faire beaucoup plus avec les CloudTrail données CloudTrail et les données.

- Renforcez la sécurité de vos données de randonnée. CloudTrailapplique automatiquement un certain niveau de sécurité lorsque vous créez un parcours. Toutefois, il existe des étapes supplémentaires que vous pouvez suivre pour aider à préserver la sécurité de vos données.
  - Par défaut, le compartiment Amazon S3 que vous avez créé dans le cadre de la création d'un suivi est soumis CloudTrail à une politique qui permet d'écrire des fichiers journaux dans ce compartiment. Le compartiment n'est pas accessible au public, mais il est possible qu'il soit accessible aux autres utilisateurs de votre AWS compte s'ils sont autorisés à lire et à écrire dans les compartiments de votre AWS compte. Examinez la politique d'accès à votre compartiment et, le cas échéant, modifiez-la pour en restreindre l'accès. Pour plus d'informations, consultez la documentation de sécurité Amazon S3 et l'exemple de démonstration relative à la sécurisation d'un compartiment.
  - Les fichiers journaux envoyés par CloudTrail votre compartiment sont chiffrés par chiffrement côté serveur Amazon avec des clés de chiffrement gérées par Amazon S3 (SSE-S3). Pour fournir une couche de sécurité directement gérable, vous pouvez plutôt utiliser le chiffrement côté serveur avec des clés AWS KMS gérées (SSE-KMS) pour vos fichiers journaux. CloudTrail Pour utiliser SSE-KMS avec CloudTrail, vous devez créer et gérer une clé KMS, également appelée. AWS KMS key Pour plus d'informations, consultez Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS).
  - Pour une planification de sécurité supplémentaire, consultez les meilleures pratiques de sécurité pour CloudTrail.
- Create a trail to log data events. (Créez un journal de suivi pour journaliser les événements de données.) Si vous souhaitez enregistrer lorsque des objets sont ajoutés, récupérés et supprimés dans un ou plusieurs compartiments Amazon S3, lorsque des éléments sont ajoutés, modifiés ou supprimés dans des tables DynamoDB, ou lorsqu'une ou AWS Lambda plusieurs fonctions sont invoquées, il s'agit d'événements de données. Le journal de suivi de gestion des événements que vous avez créé précédemment dans ce didacticiel ne journalise pas ces types d'événements. Vous pouvez créer un journal distinct spécifiquement pour consigner les événements de données pour certains ou tous les types de ressources pris en charge. Pour plus d'informations, consultez Événements de données.

  > **Note**
  >
  > Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour plus d'informations, consultez Tarification AWS CloudTrail.

- Enregistrez CloudTrail les événements Insights sur votre parcours. AWS CloudTrail Insights aide AWS les utilisateurs à identifier les activités inhabituelles associées aux appels d'API et aux taux d'erreur des API et à y répondre en analysant en permanence les événements CloudTrail de gestion. CloudTrail Insights utilise des modèles mathématiques pour déterminer les niveaux normaux d'activité des API et des événements de service pour un compte. Il identifie les comportements qui sortent des modèles normaux, génère des événements Insights et transmet ces événements à un dossier `/CloudTrail-Insight` dans le compartiment S3 de destination choisi pour votre journal de suivi. Pour plus d'informations sur CloudTrail Insights, consultezJournalisation des événements Insights.

  > **Note**
  >
  > Des frais supplémentaires s'appliquent pour la journalisation des événements Insights. Pour plus d'informations, consultez Tarification AWS CloudTrail.

- Configurez CloudWatch les alarmes Logs pour vous avertir lorsque certains événements se produisent. CloudWatch Les journaux vous permettent de surveiller et de recevoir des alertes pour des événements spécifiques capturés par CloudTrail. Par exemple, il est possible de contrôler des événements clés liés à la sécurité et au réseau, tels que modifications de groupes de sécurité, échec des événements de connexion à AWS Management Console, ou modifications apportées aux politiques IAM. Pour plus d'informations, consultez Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.
- Utilisez des outils d'analyse pour identifier les tendances dans vos CloudTrail journaux. Bien que les filtres dans l'historique d'événements puissent vous aider à trouver des événements spécifiques ou des types d'événements dans votre activité récente, ils ne fournissent pas la possibilité de rechercher dans l'activité sur de plus longues périodes. Pour une analyse plus approfondie et plus sophistiquée, vous pouvez utiliser Amazon Athena. Pour plus d'informations, consultez la section Interrogation des AWS CloudTrail journaux dans le guide de l'utilisateur d'Amazon Athena.

Création d'un magasin de données d'événements pour les événements de données S3

Vous pouvez créer un magasin de données d'événements pour enregistrer les CloudTrail événements (événements de gestion, événements de données), les événements CloudTrail Insights, les AWS Audit Manager preuves, les éléments de AWS Config configuration ou les AWS non-événements.

Lorsque vous créez un magasin de données d'événements pour les événements de données, vous choisissez les types de ressources Services AWS et les types de ressources pour lesquels vous souhaitez enregistrer les événements de données. Pour plus d'informations sur Services AWS les événements liés aux données de ce journal, consultezÉvénements de données.

Cette procédure pas à pas explique comment créer un magasin de données d'événements pour les événements de données Amazon S3. Dans ce didacticiel, au lieu de journaliser tous les événements liés aux données Amazon S3, nous allons choisir un modèle de sélecteur de journal personnalisé pour ne journaliser les événements que lorsqu'un objet est supprimé d'un compartiment S3 spécifique.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Pour créer un magasin de données d'événement pour des événements S3

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configurer le magasin de données d'événements, dans Détails généraux, donnez un nom à votre magasin de données d'événements, tel que *s3- data-events-eds*. Comme bonne pratique, utilisez un nom qui identifie rapidement l'objectif de l'entrepôt de données d'événement. Pour plus d'informations sur les exigences en matière de CloudTrail dénomination, consultezExigences de dénomination.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

- Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
  - Période de conservation par défaut : 366 jours.
  - Période de conservation maximale : 3 653 jours
- Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
  - Période de conservation par défaut : 2 557 jours.
  - Période de conservation maximale : 2 557 jours

6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

7. (Facultatif) Dans Chiffrement, indiquez si vous souhaitez chiffrer l'entrepôt de données d'événement à l'aide de votre propre clé KMS. Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés CloudTrail à l'aide d'une clé AWS KMS détenue et gérée pour vous.

   Pour activer le chiffrement à l'aide de votre propre clé KMS, choisissez Utiliser ma propre AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour

plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

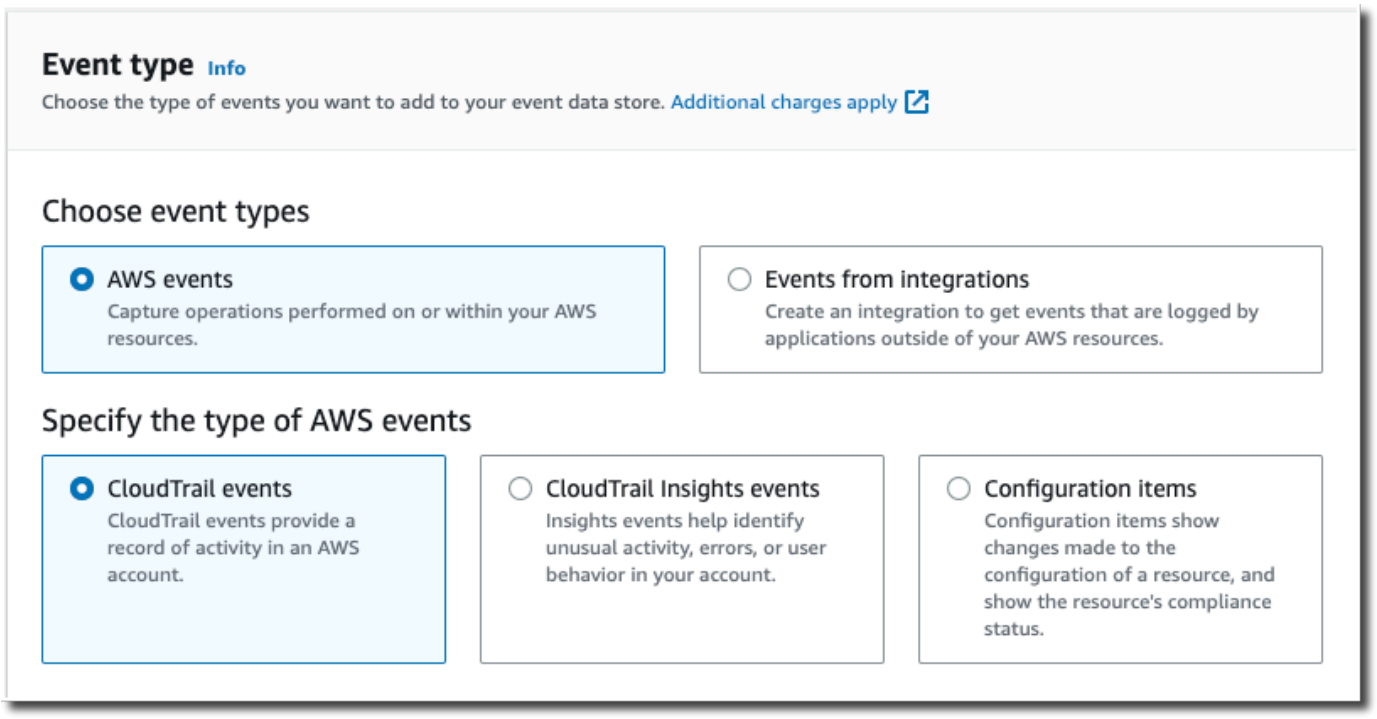
   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans Balises, ajoutez une ou plusieurs identifications personnalisées (paires valeur-clé) à votre magasin de données d'événement. Les balises peuvent vous aider à identifier les magasins de données de vos CloudTrail événements. Par exemple, il est possible d'attacher une balise portant le nom **`stage`** à la valeur **`prod`**. Vous pouvez utiliser des balises pour limiter

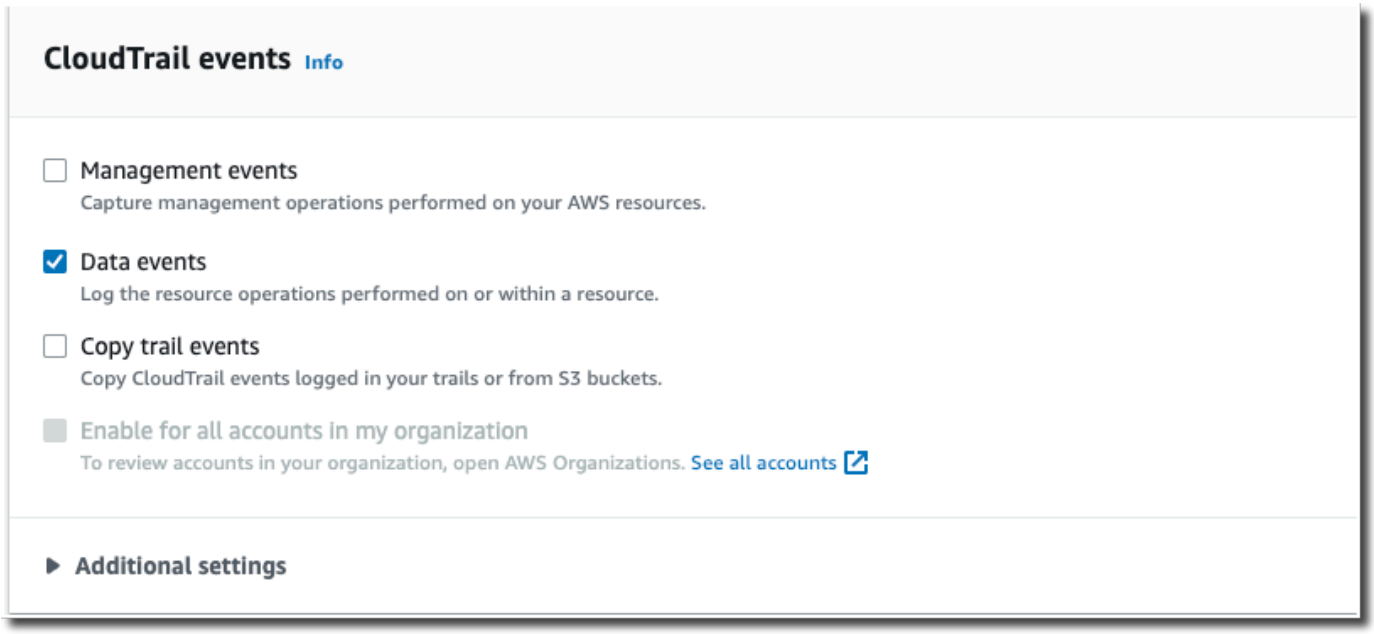
l'accès à votre entrepôt de données d'événement. Vous pouvez également utiliser des balises pour suivre les coûts de requête et d'ingestion pour votre entrepôt de données d'événement.

Pour plus d'informations sur l'utilisation des balises pour le suivi des coûts, veuillez consulter Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un entrepôt de données d'événement basé sur des balises, veuillez consulter Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

10. Choisissez Suivant pour configurer le magasin de données d'événement.
11. Sur la page Choisir des événements, conservez les sélections par défaut pour Type d'événement.



12. Pour les CloudTrail événements, choisissez Data events et désélectionnez Management events. Pour plus d'informations sur les événements de données, veuillez consulter Journalisation des événements de données.



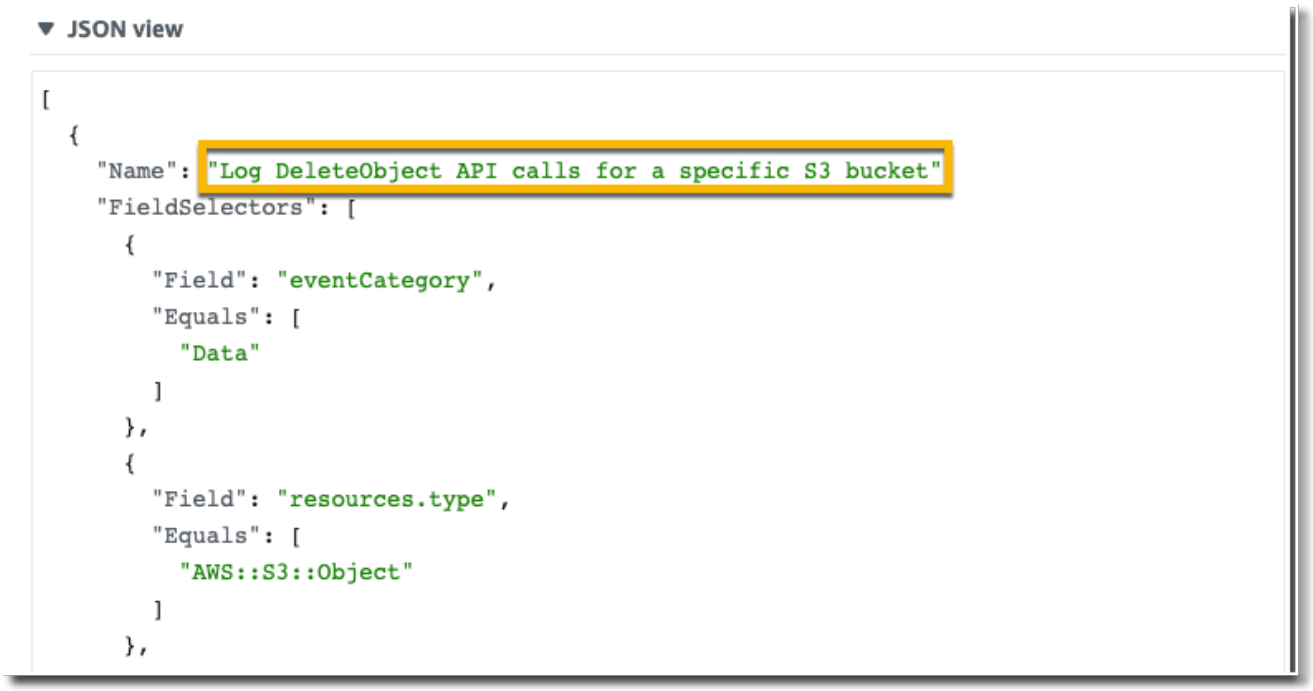
13. Conservez le paramètre par défaut pour Copier les événements de suivi. Vous utiliseriez cette option pour copier des événements de journal de suivi existant dans votre entrepôt de données d'événement. Pour plus d'informations, consultez Copier des événements de journal de suivi dans un magasin de données d'événement.
14. Choisissez Activer pour tous les comptes de mon organisation s'il s'agit d'un entrepôt de données d'événement d'organisation. Cette option ne pourra pas être modifiée à moins que vous ayez des comptes configurés dans AWS Organizations.
15. Pour Paramètres supplémentaires, laissez les sélections par défaut. Par défaut, un magasin de données d'événements collecte les événements pour tous Régions AWS et commence à les ingérer dès sa création.
16. Pour Événements de données, effectuez les sélections suivantes :

    a. Dans Type d'événement de données, choisissez S3. Le type d'événement de données identifie la ressource Service AWS et la ressource sur laquelle les événements de données sont enregistrés.

    b. Dans Modèle de sélecteur de journaux, choisissez Personnalisé. En choisissant Personnalisé, vous pouvez définir un sélecteur d'événements personnalisé pour filtrer les champs `eventName`, `resources.ARN` et `readOnly`. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelectorla référence de l'AWS CloudTrail API.

    c. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est le nom descriptif d'un sélecteur d'événements avancé, tel que « Log DeleteObject API calls for a specific S3 bucket ». Le nom du sélecteur est répertorié comme

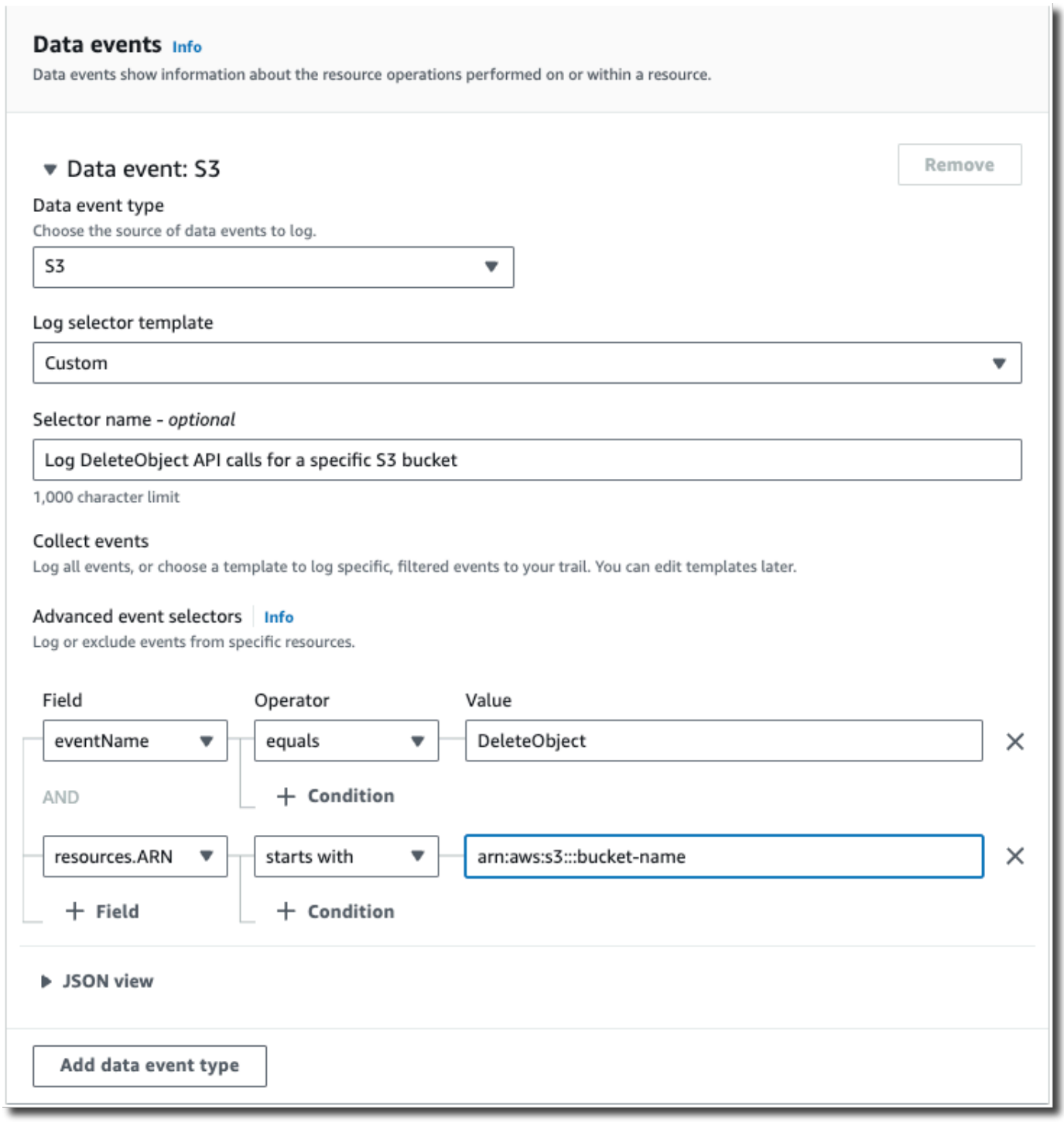
Name dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.



d. Dans les sélecteurs d'événements avancés, nous allons créer le sélecteur d'événements personnalisé pour filtrer les champs `eventName` et`resources.`ARN. Les sélecteurs d'événements avancés pour un magasin de données d'événement fonctionnent de la même manière que les sélecteurs d'événements avancés que vous appliquez à un journal de suivi. Pour plus d'informations sur la création de sélecteurs d'événements avancés, consultez Journalisation des événements de données à l'aide de sélecteurs d'événement avancés.

   i. Pour Champ, choisissez eventName. Pour Opérateur, choisissez Égal à. Pour le champ Valeur, saisissez **`DeleteObject`**. Choisissez + Champ pour filtrer sur un autre champ.

   ii. Pour Champ, choisissez resources.ARN. Pour Opérateur, choisissez StartsWith. Pour Value, saisissez l'ARN de votre compartiment (par exemple, *`arn:aws:s3:::bucket-name`*). Pour plus d'informations sur la façon d'obtenir l'ARN, veuillez consulter les ressources Amazon S3 dans le Guide de l'utilisateur d'Amazon Simple Storage Service.



17. Choisissez Suivant pour examiner vos préférences.
18. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.

19. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

    À partir de ce moment, le magasin de données d'événement capture les événements qui correspondent à ses sélecteurs d'événements avancés. Les événements s'étant produits avant la création du stockage de données d'événement ne figurent pas dans celui-ci, à moins que vous ne choisissiez de copier les événements de suivi existants.

Vous pouvez désormais exécuter des requêtes sur votre entrepôt de données d'événement. Pour plus d'informations sur la façon d'afficher et d'exécuter des exemples de requêtes, veuillez consulter Afficher et exécuter des exemples de requêtes CloudTrail Lake.

Copier les événements du parcours dans un magasin de données d'événements CloudTrail Lake

Cette procédure pas à pas vous explique comment copier des événements de parcours dans un nouveau magasin de données d'événements CloudTrail Lake à des fins d'analyse historique. Pour plus d'informations sur la copie d'événements de journal de suivi, veuillez consulter Copier des événements de journal de suivi dans un magasin de données d'événement.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Lorsque vous copiez des événements de parcours dans un magasin de données d'événements CloudTrail Lake, vous êtes facturé en fonction de la quantité de données non compressées ingérée par le magasin de données d'événements.

Lorsque vous copiez des événements de suivi dans CloudTrail Lake, CloudTrail décompressez les journaux stockés au format gzip (compressé), puis copie les événements contenus dans les journaux dans votre magasin de données d'événements. La taille des données non compressées peut être supérieure à la taille réelle du stockage S3. Pour obtenir une estimation générale de la taille des données non compressées, vous pouvez multiplier par 10 la taille des journaux du compartiment S3.

Vous pouvez réduire les coûts en spécifiant une plage de temps plus restreinte pour les événements copiés. Si vous prévoyez de n'utiliser l'entrepôt de données d'événement que pour interroger vos événements copiés, vous pouvez désactiver l'ingestion des événements afin d'éviter d'encourir des frais lors d'événements futurs. Pour plus d'informations sur les coûts, consultez la section AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Pour copier des événements de journal de suivi dans un entrepôt de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configurer le magasin de données d'événements, dans Détails généraux, donnez un nom à votre magasin de données d'événements, tel que *my-management-events-eds*. Comme bonne pratique, utilisez un nom qui identifie rapidement l'objectif de l'entrepôt de données d'événement. Pour plus d'informations sur les exigences en matière de CloudTrail dénomination, consultezExigences de dénomination.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
     - Période de conservation par défaut : 366 jours.
     - Période de conservation maximale : 3 653 jours
   - Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.

- Période de conservation par défaut : 2 557 jours.
- Période de conservation maximale : 2 557 jours

6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

   > **Note**
   >
   > Si vous copiez des événements de suivi dans cette banque de données d'événements, vous ne CloudTrail copierez aucun événement s'il `eventTime` est antérieur à la période de conservation spécifiée. Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.

7. (Facultatif) Dans Chiffrement, indiquez si vous souhaitez chiffrer l'entrepôt de données d'événement à l'aide de votre propre clé KMS. Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés CloudTrail à l'aide d'une clé AWS KMS détenue et gérée pour vous.

   Pour activer le chiffrement à l'aide de votre propre clé KMS, choisissez Utiliser ma propre AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour

plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

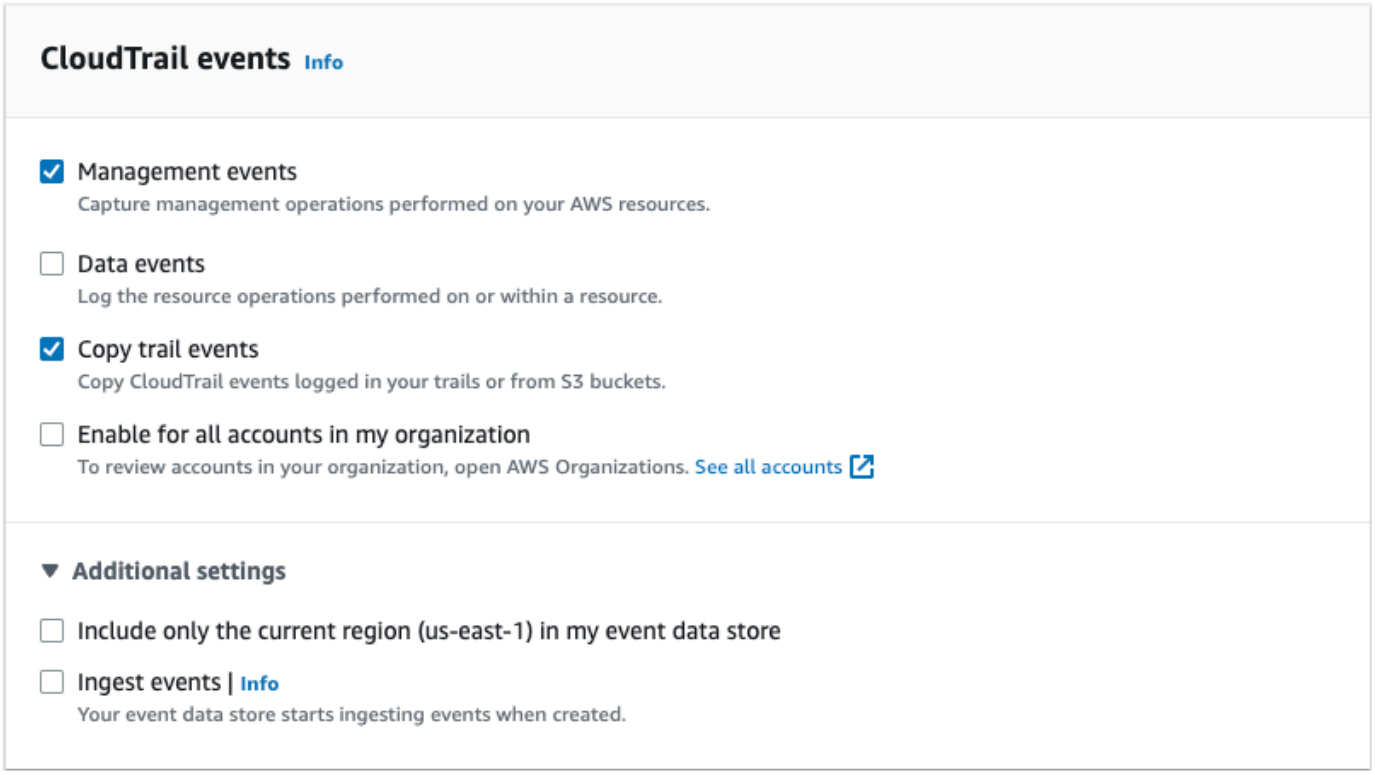
9. (Facultatif) Dans Balises, ajoutez une ou plusieurs identifications personnalisées (paires valeur-clé) à votre magasin de données d'événement. Les balises peuvent vous aider à identifier les magasins de données de vos CloudTrail événements. Par exemple, il est possible d'attacher une balise portant le nom **`stage`** à la valeur **`prod`**. Vous pouvez utiliser des balises pour limiter

l'accès à votre entrepôt de données d'événement. Vous pouvez également utiliser des balises pour suivre les coûts de requête et d'ingestion pour votre entrepôt de données d'événement.

Pour plus d'informations sur l'utilisation des balises pour le suivi des coûts, veuillez consulter Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un entrepôt de données d'événement basé sur des balises, veuillez consulter Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

10. Choisissez Suivant pour configurer le magasin de données d'événement.
11. Sur la page Choisir des événements, conservez les sélections par défaut pour Type d'événement.
12. Pour les CloudTrail événements, nous laisserons les événements de gestion sélectionnés et choisirons Copier les événements de piste. Dans cet exemple, les types d'événements ne nous intéressent pas, car nous n'utilisons l'entrepôt de données d'événement que pour analyser les événements passés et non pour ingérer les événements futurs.

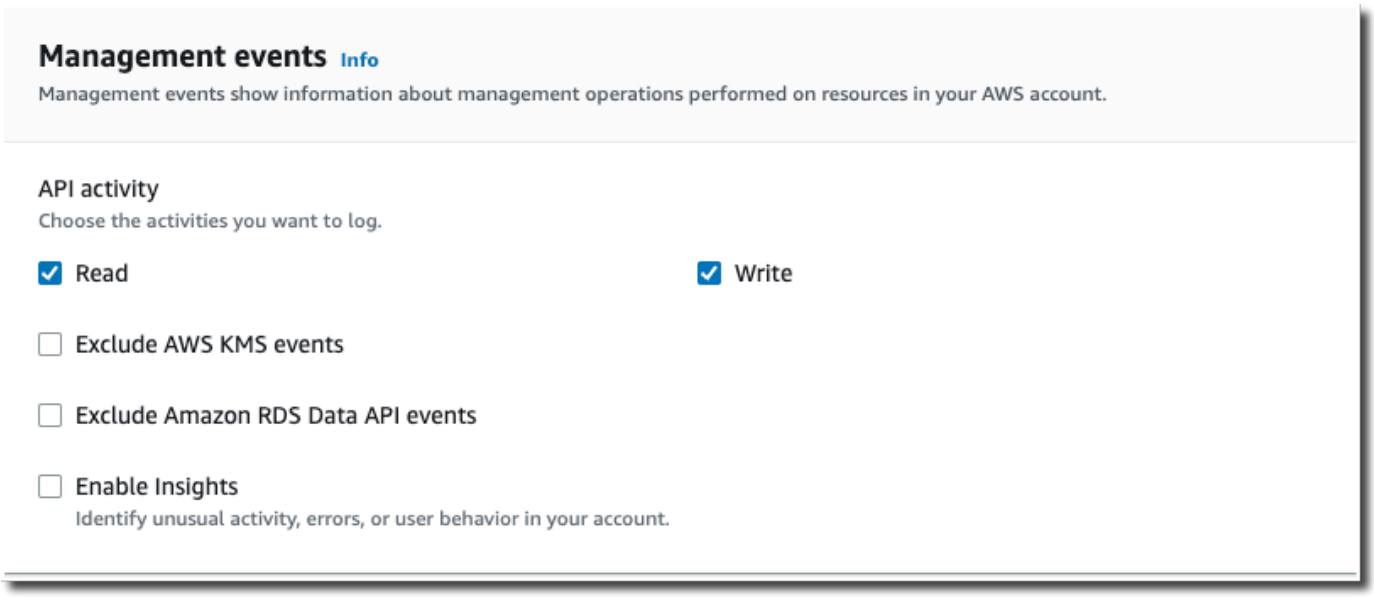
    Si vous créez un entrepôt de données d'événement pour remplacer un journal de suivi existant, choisissez les mêmes sélecteurs d'événements que votre journal de suivi pour vous assurer que l'entrepôt de données d'événement couvre les mêmes événements.



13. Choisissez Activer pour tous les comptes de mon organisation s'il s'agit d'un entrepôt de données d'événement d'organisation. Cette option ne pourra pas être modifiée à moins que vous ayez des comptes configurés dans AWS Organizations.

> **Note**
>
> Si vous créez un entrepôt de données d'événement d'organisation, vous devez être connecté avec le compte de gestion de l'organisation, car seul celui-ci peut copier les événements de journal de suivi vers l'entrepôt de données d'événement d'organisation.

14. Pour Paramètres supplémentaires, nous allons désélectionner Ingérer les événements, car dans cet exemple, nous ne voulons pas que l'entrepôt de données d'événement ingère des événements futurs, puisque nous ne sommes intéressés que par l'interrogation des événements copiés. Par défaut, un magasin de données d'événements collecte les événements pour tous Régions AWS et commence à les ingérer dès sa création.
15. Pour Événements de gestion, nous conserverons les paramètres par défaut.



16. Dans la zone Copier les événements du journal de suivi, effectuez les étapes suivantes.

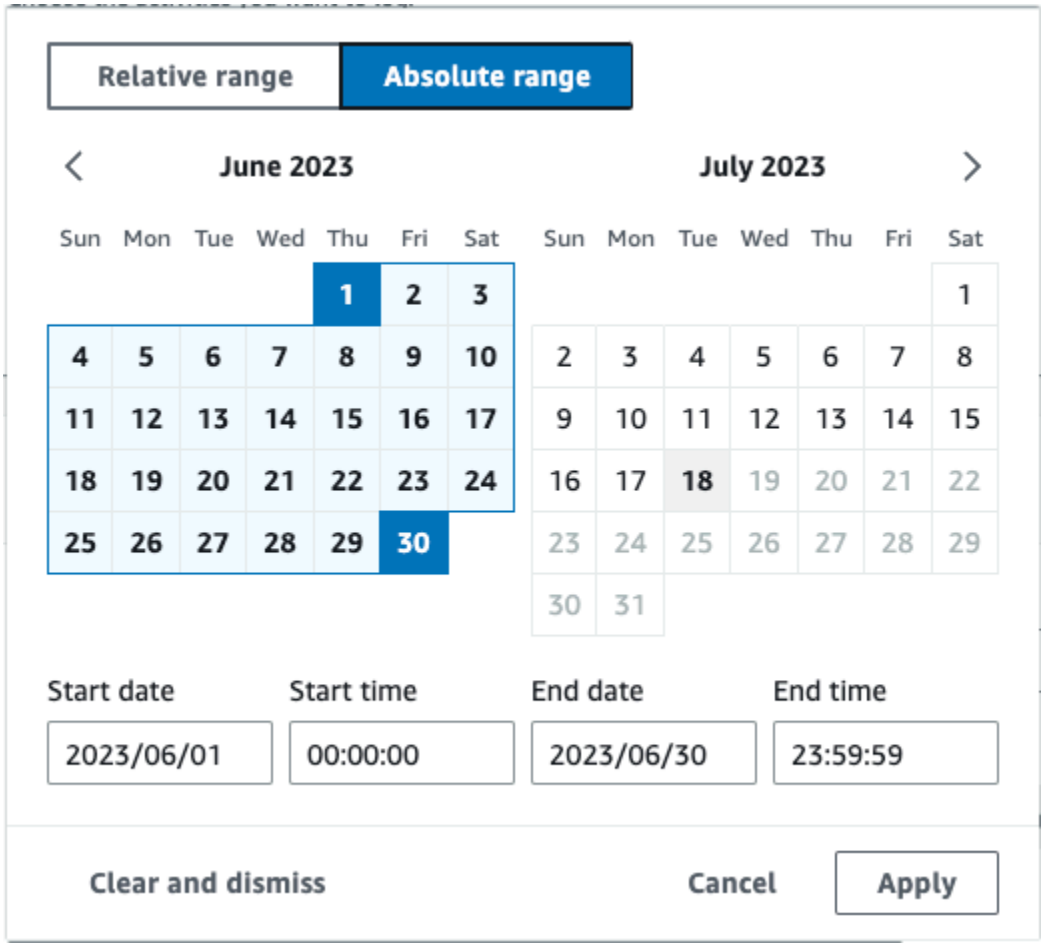
    a. Sélectionnez le journal de suivi que vous voulez copier. Dans cet exemple, nous allons choisir un journal de suivi nommé *`management-events`*.

       Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, choisissez Enter S3 URI, puis Browse S3 pour accéder au préfixe. Si le compartiment S3 source pour le suivi utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique en matière de clés KMS autorise CloudTrail le déchiffrement des données. Si votre compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé afin de CloudTrail permettre le déchiffrement des données du compartiment. Pour plus d'informations sur la mise à jour de la stratégie de clé KMS, veuillez consulter Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source.

    b. Choisissez un intervalle de temps pour copier les événements. CloudTrail vérifie le préfixe et le nom du fichier journal pour vérifier que le nom contient une date comprise entre les dates de début et de fin choisies avant de tenter de copier les événements de suivi. Vous avez le choix entre Plage relative ou Plage absolue. Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez une plage de temps antérieure à la création du magasin de données d'événement.

- Si vous choisissez Plage relative, vous pouvez choisir de copier les événements enregistrés au cours des 6 derniers mois, 1 an, 2 ans, 7 ans ou une plage personnalisée. CloudTrail copie les événements enregistrés pendant la période choisie.
- Si vous choisissez la plage absolue, vous pouvez choisir une date de début et une date de fin spécifiques. CloudTrail copie les événements survenus entre les dates de début et de fin choisies.

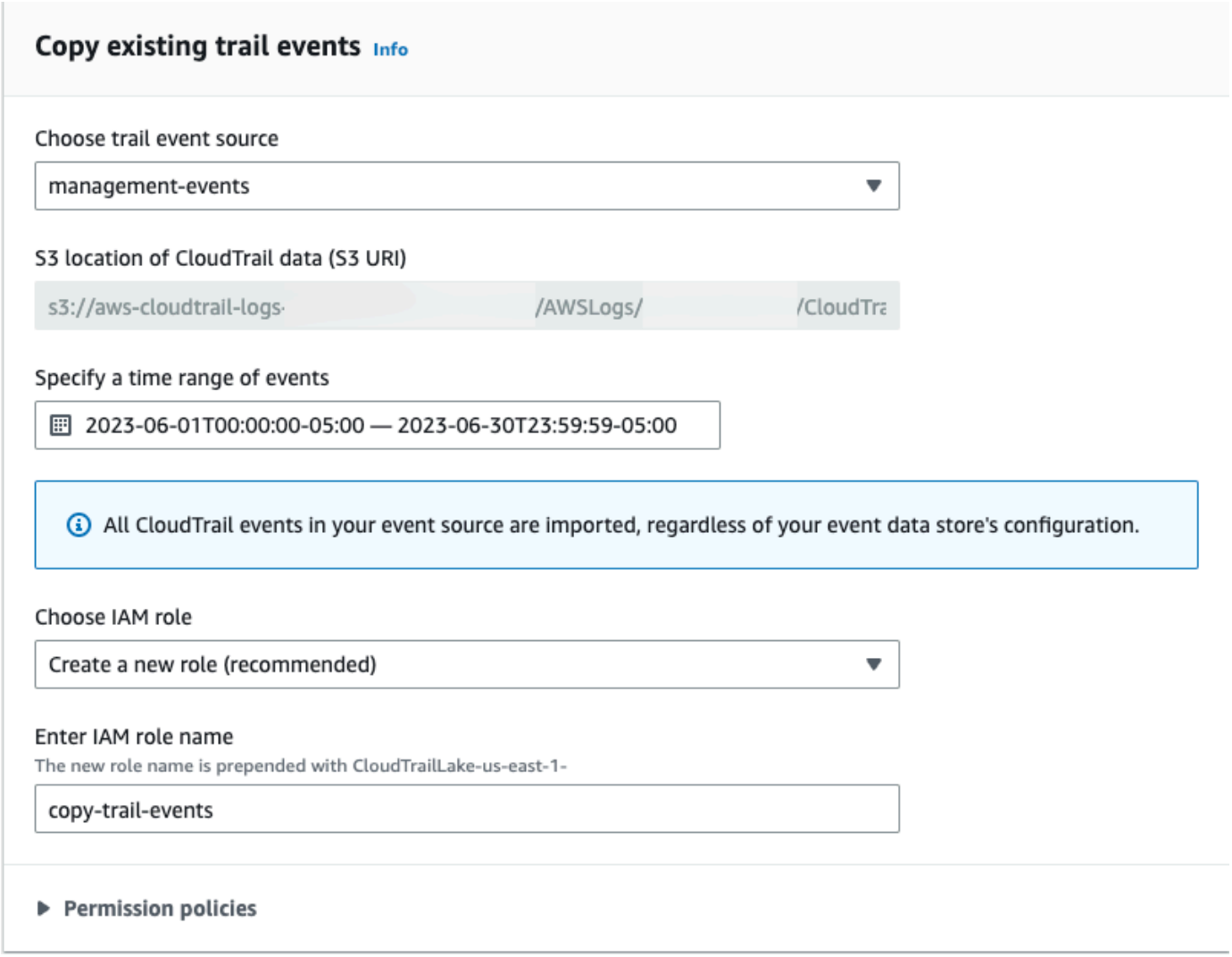
Dans cet exemple, nous allons choisir Plage absolue et nous allons sélectionner l'ensemble du mois de juin.



c. Pour Autorisations, sélectionnez l'une des options de rôle IAM suivantes. Si vous choisissez un rôle IAM existant, vérifiez que la politique de rôle IAM fournit les autorisations nécessaires. Pour plus d'informations sur la mise à jour des autorisations du rôle IAM, consultez Autorisations IAM pour copier les événements de journal de suivi.

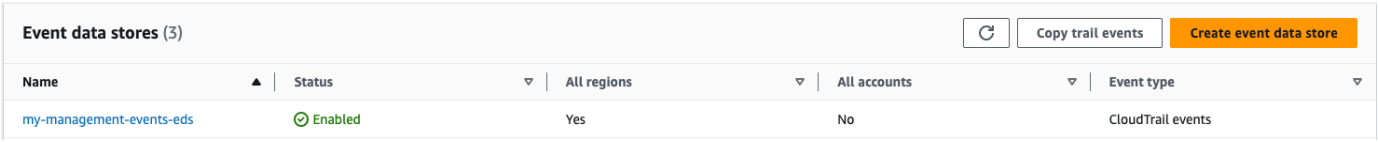
- Sélectionnez Créer un nouveau rôle (recommandé) pour créer un nouveau rôle IAM. Pour Enter IAM role name, saisissez le nom du rôle. CloudTrailcrée automatiquement les autorisations nécessaires pour ce nouveau rôle.
- Choisissez Utiliser un ARN de rôle IAM personnalisé pour utiliser un rôle IAM personnalisé qui n'est pas répertorié. Pour Enter IAM role ARN (Saisir l'ARN du rôle IAM), saisissez l'ARN IAM.
- Choisissez un rôle IAM existant dans la liste déroulante.

Dans cet exemple, nous choisirons Créer un nouveau rôle (recommandé) et nous fournirons le nom **`copy-trail-events`**.



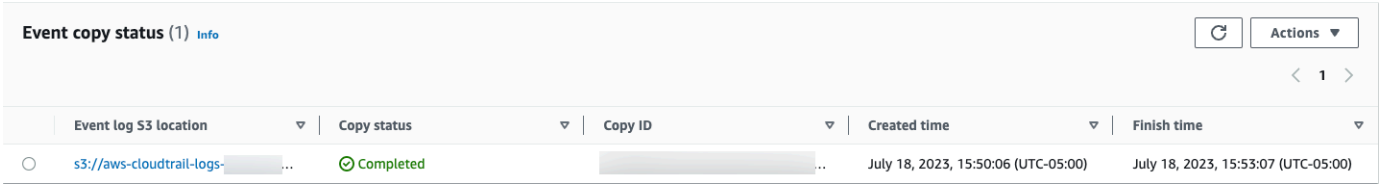
17. Choisissez Suivant pour examiner vos préférences.

18. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
19. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

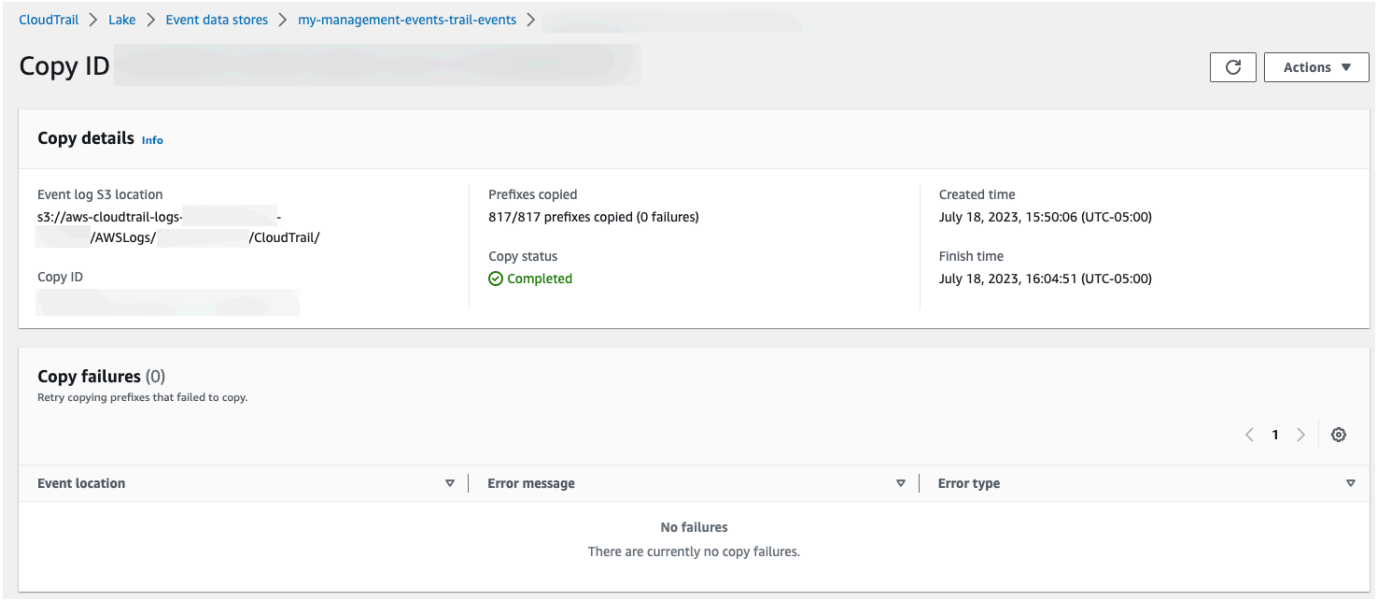


20. Choisissez le nom de l'entrepôt de données d'événement pour afficher la page contenant ses détails. La page de détails indique les détails de votre entrepôt de données d'événement et le statut de la copie. L'état de la copie d'événement est affiché dans la zone État de la copie d'événement.

    Lorsque la copie d'un événement de journal de suivi est terminée, son Statut de la copie est défini sur Terminé si aucune erreur n'est survenue, ou Échec si des erreurs sont survenues.



21. Pour afficher plus de détails sur la copie, choisissez le nom de la copie dans la colonne Emplacement S3 du journal des événements ou choisissez l'option Afficher les détails dans le menu Actions. Pour plus d'informations sur l'affichage des informations relatives à la copie d'un événement de journal de suivi, veuillez consulter Informations de copie d'événement.



22. La zone Échecs de copie indique toutes les erreurs survenues lors de la copie des événements de suivi. Si le Statut de la copie est Échec, corrigez les erreurs qui s'affichent dans Échecs de la copie, puis sélectionnez Réessayer la copie. Lorsque vous réessayez d'effectuer une copie, elle CloudTrail reprend à l'endroit où l'échec s'est produit.

Afficher les tableaux de bord de CloudTrail Lake

Cette procédure pas à pas vous montre comment afficher les tableaux de bord de CloudTrail Lake. CloudTrailLes tableaux de bord Lake vous permettent de visualiser les événements dans votre banque de données d'événements et de voir les tendances, telles que les principaux utilisateurs et les principales erreurs.

Chaque tableau de bord est composé de plusieurs widgets et chaque widget représente une requête SQL. Pour remplir le tableau de bord, CloudTrail exécute des requêtes générées par le système. Les requêtes sont facturées en fonction de la quantité de données analysées.

> **Note**
>
> Actuellement, les tableaux de bord ne sont disponibles que pour les magasins de données d'événements qui collectent CloudTrail des événements de gestion, des événements de données Amazon S3 et des événements Insights.

Pour consulter les tableaux de bord Lake

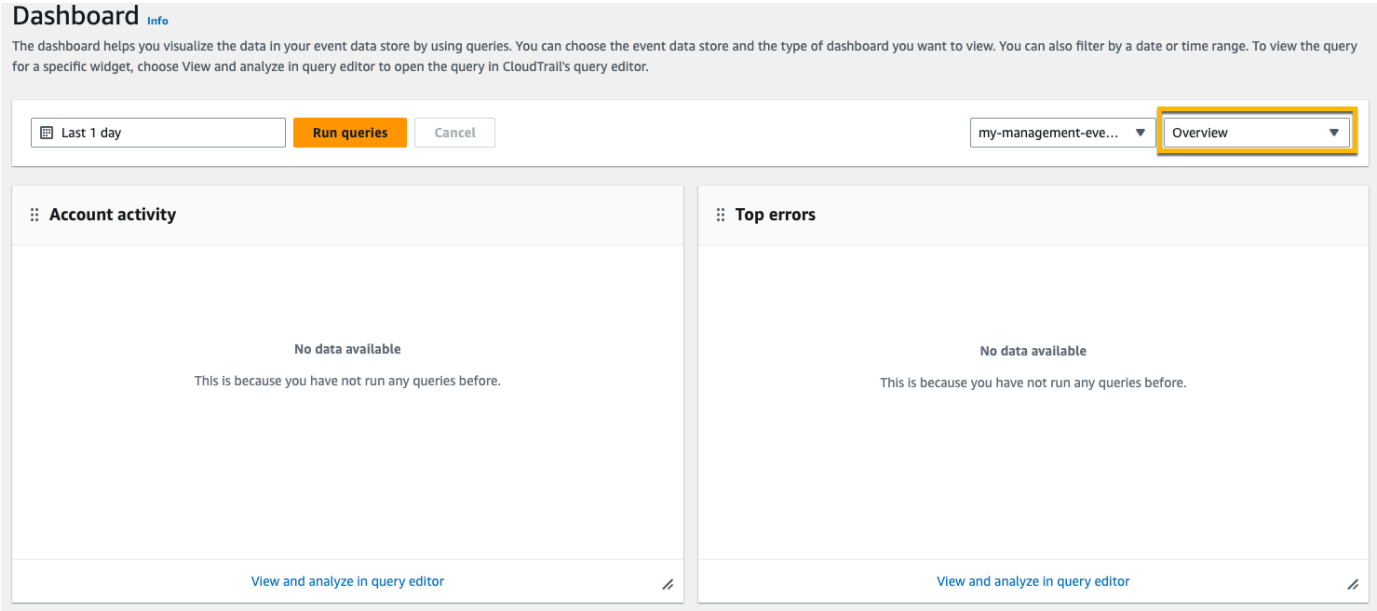
1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Tableau de bord.
3. La première fois que vous consultez la page Tableaux de bord, il vous CloudTrail est demandé de confirmer les coûts associés à l'exécution des requêtes. Choisissez J'accepte de prendre en charge les frais d'exécution des requêtes. Il s'agit d'une confirmation unique. Pour plus d'informations sur la CloudTrail tarification, consultez la section CloudTrailTarification.
4. Choisissez votre entrepôt de données d'événement dans la liste, puis choisissez le type de tableau de bord que vous souhaitez consulter.

   Les types de tableaux de bord possibles sont les suivants.

- Tableau de bord d'ensemble : affiche les utilisateurs les plus actifs Régions AWS, et Services AWS par nombre d'événements. Vous pouvez également consulter des informations sur l'activité des événements de gestion `read` et `write`, les événements les plus limités et les principales erreurs. Ce tableau de bord est disponible pour les entrepôts de données d'événement qui collectent des événements de gestion.
- Tableau de bord Événements de gestion : affiche les événements de connexion à la console, les événements de refus d'accès, les actions destructrices et les principales erreurs par utilisateur. Vous pouvez également consulter des informations sur les versions TLS et les appels TLS périmés par utilisateur. Ce tableau de bord est disponible pour les entrepôts de données d'événement qui collectent des événements de gestion.
- Tableau de bord Événements de données S3 : affiche l'activité du compte S3, les objets S3 les plus consultés, les principaux utilisateurs S3 et les principales actions S3. Ce tableau de bord est disponible pour les entrepôts de données d'événement qui collectent des événements de données Amazon S3.
- Tableau de bord Événements Insights : affiche la proportion globale d'événements Insights par type Insights, la proportion d'événements Insights par type Insights pour les principaux utilisateurs et services, et le nombre d'événements Insights par jour. Le tableau de bord inclut également un widget qui répertorie jusqu'à 30 jours d'événements Insights. Ce tableau de bord n'est disponible que pour les entrepôts de données d'événement qui collectent des événements Insights.

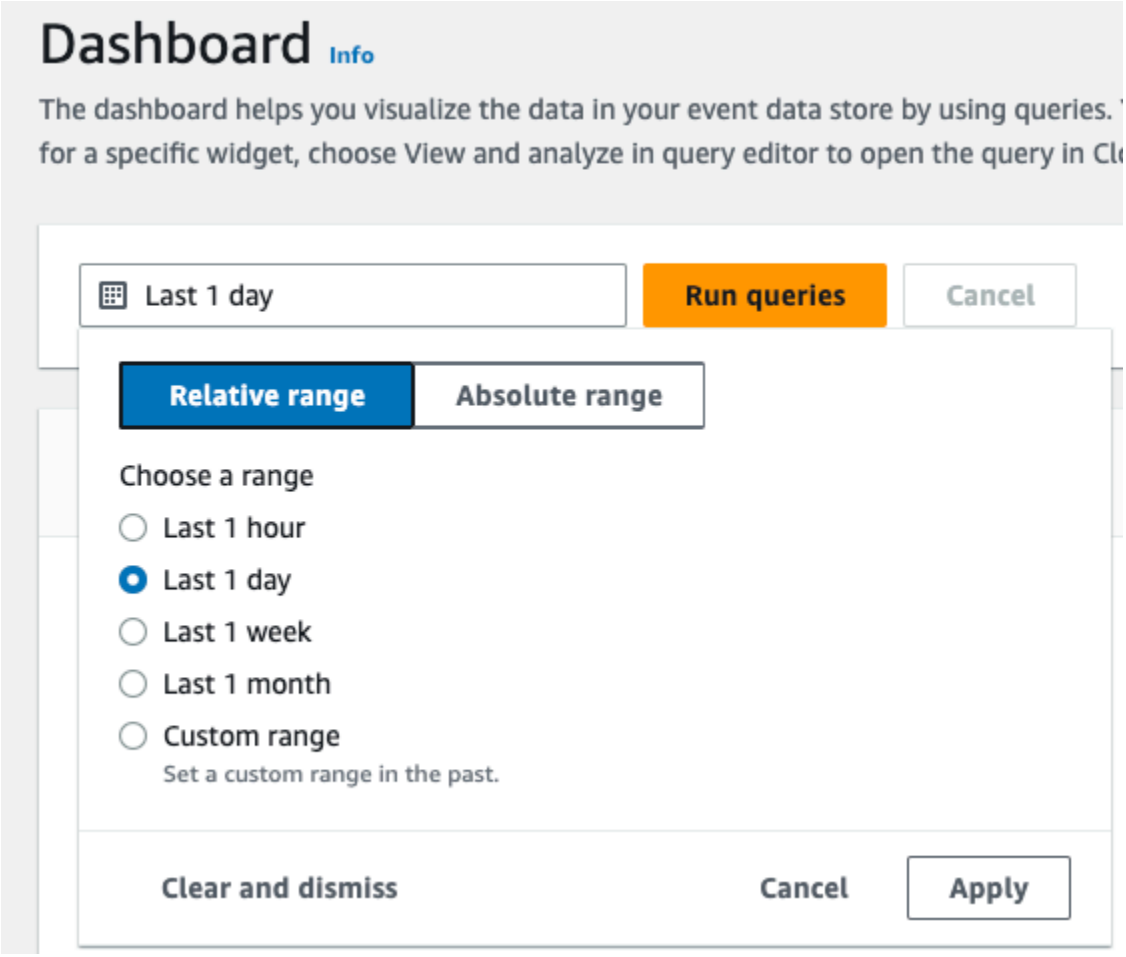
> **Note**
>
> - Une fois que vous avez activé CloudTrail Insights pour la première fois dans le magasin de données d'événements source, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée. Pour plus d'informations, consultez Comprendre la diffusion d'événements Insights.
> - Le tableau de bord Événements Insights n'affiche que les informations relatives aux événements Insights collectés par l'entrepôt de données d'événement sélectionné, qui sont déterminées par la configuration de l'entrepôt de données d'événement source. Par exemple, si vous configurez l'entrepôt de données d'événement source pour activer les événements Insights `ApiCallRateInsight`, mais pas `ApiErrorRateInsight`, vous ne verrez aucune information sur les événements Insights sur `ApiErrorRateInsight`.

Dans cet exemple, nous avons choisi le tableau de bord Présentation.



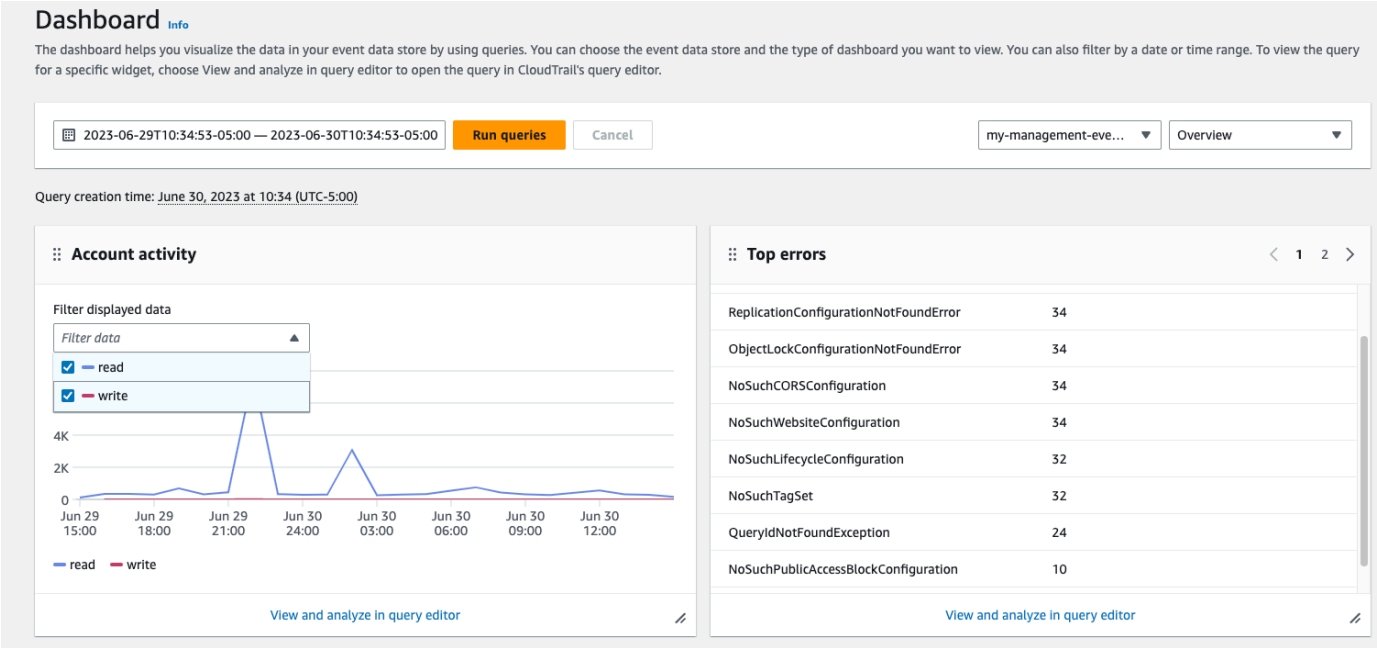
5. Choisissez le champ de date pour filtrer sur une plage horaire, puis sélectionnez Appliquer. Choisissez Plage absolue pour sélectionner une plage de dates et d'heures spécifique. Choisissez Plage relative pour sélectionner une plage de temps prédéfinie ou une plage personnalisée. Par défaut, le tableau de bord affiche les données des événements des dernières 24 heures.

> **Note**
>
> Les CloudTrail requêtes étant facturées en fonction de la quantité de données numérisées, vous pouvez réduire les coûts en filtrant sur une plage de temps plus étroite.

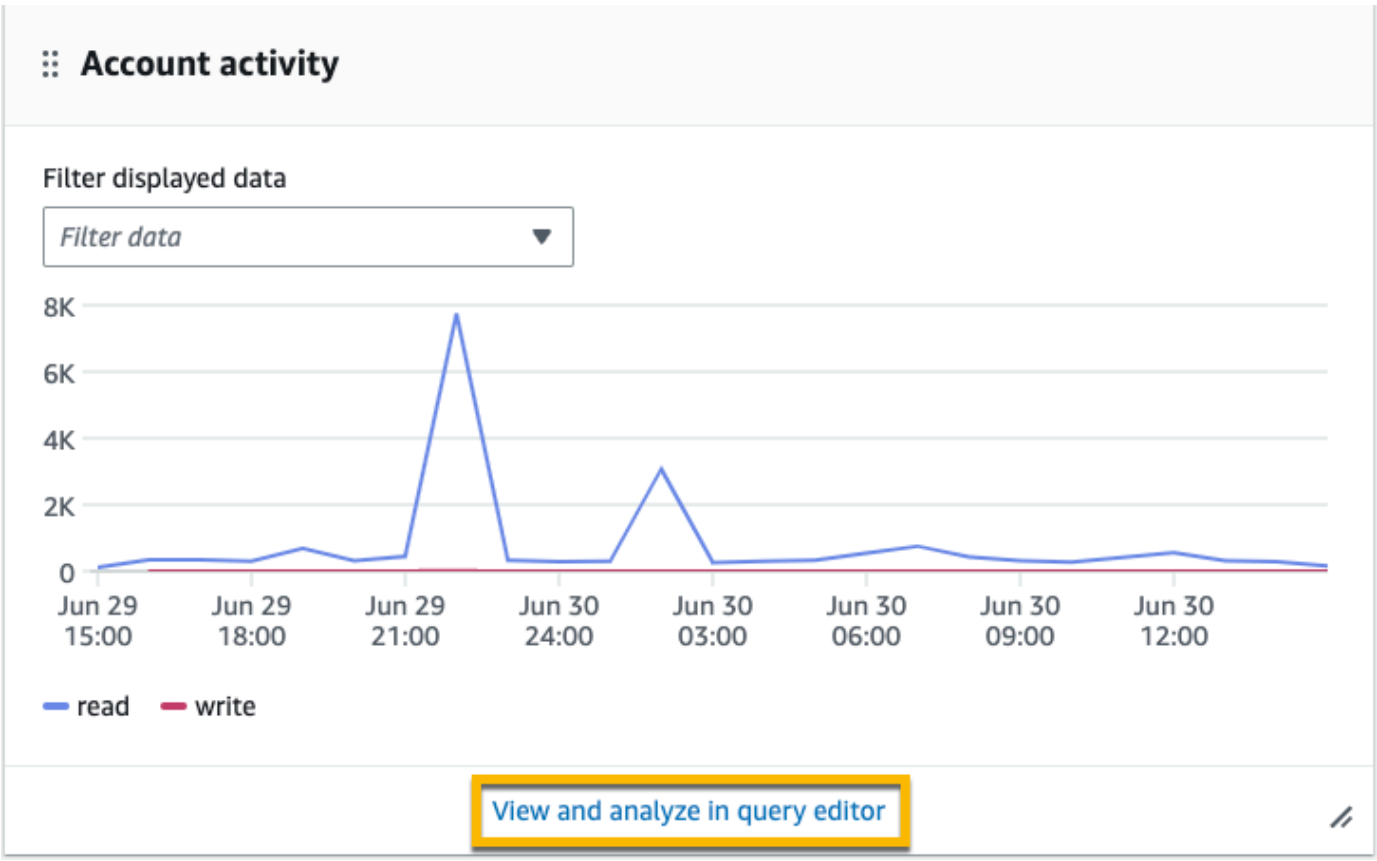


6. Choisissez Exécuter les requêtes pour remplir le tableau de bord. Chaque widget affiche individuellement le statut de la requête associée et présente les données une fois la requête terminée.

   Vous pouvez effectuer un filtrage supplémentaire sur certains widgets, tels que l'Activité du compte, qui vous permet de filtrer l'activité des événements `read` et `write`.

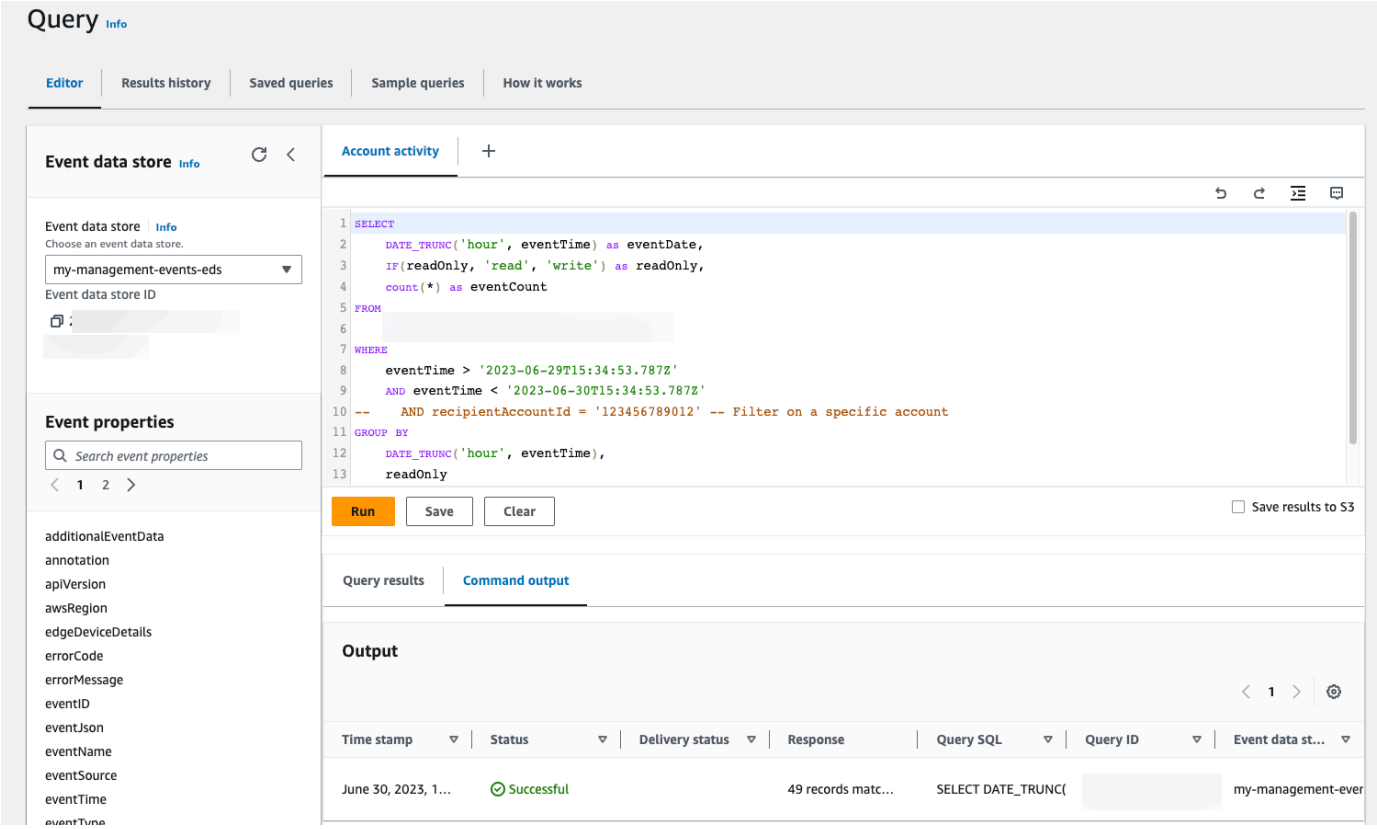


7. Pour afficher la requête d'un widget, choisissez Afficher et analyser dans l'éditeur de requêtes.



Choisir Afficher et analyser dans l'éditeur de requêtes ouvre la requête dans l'éditeur de requêtes de CloudTrail Lake, ce qui vous permet d'analyser plus en détail les résultats de la requête

en dehors du tableau de bord. Pour plus d'informations sur l'édition d'une requête, veuillez consulter Créer ou modifier une requête. Pour plus d'informations sur l'exécution d'une requête et l'enregistrement des résultats, veuillez consulter Exécuter une requête et enregistrer les résultats.



Pour de plus amples informations sur les tableaux de bord, veuillez consulter Afficher les tableaux de bord de CloudTrail Lake.

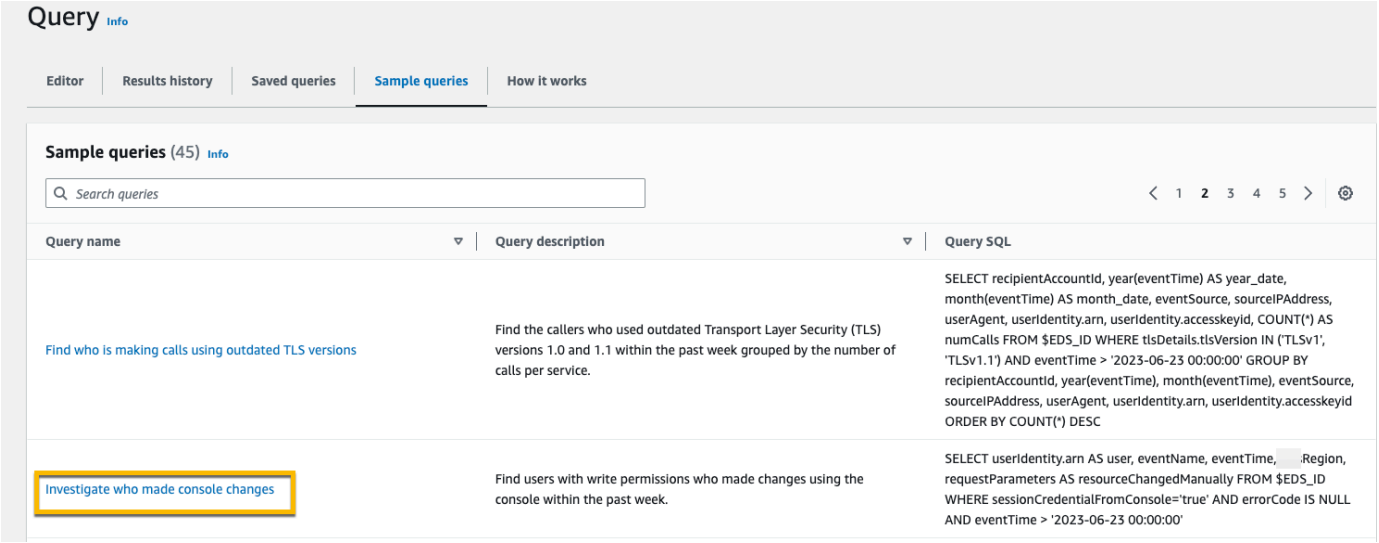
Afficher et exécuter des exemples de requêtes CloudTrail Lake

CloudTrail Lake fournit un certain nombre d'exemples de requêtes qui peuvent vous aider à commencer à écrire vos propres requêtes. Cette procédure pas à pas vous montre comment sélectionner et exécuter un exemple de requête.

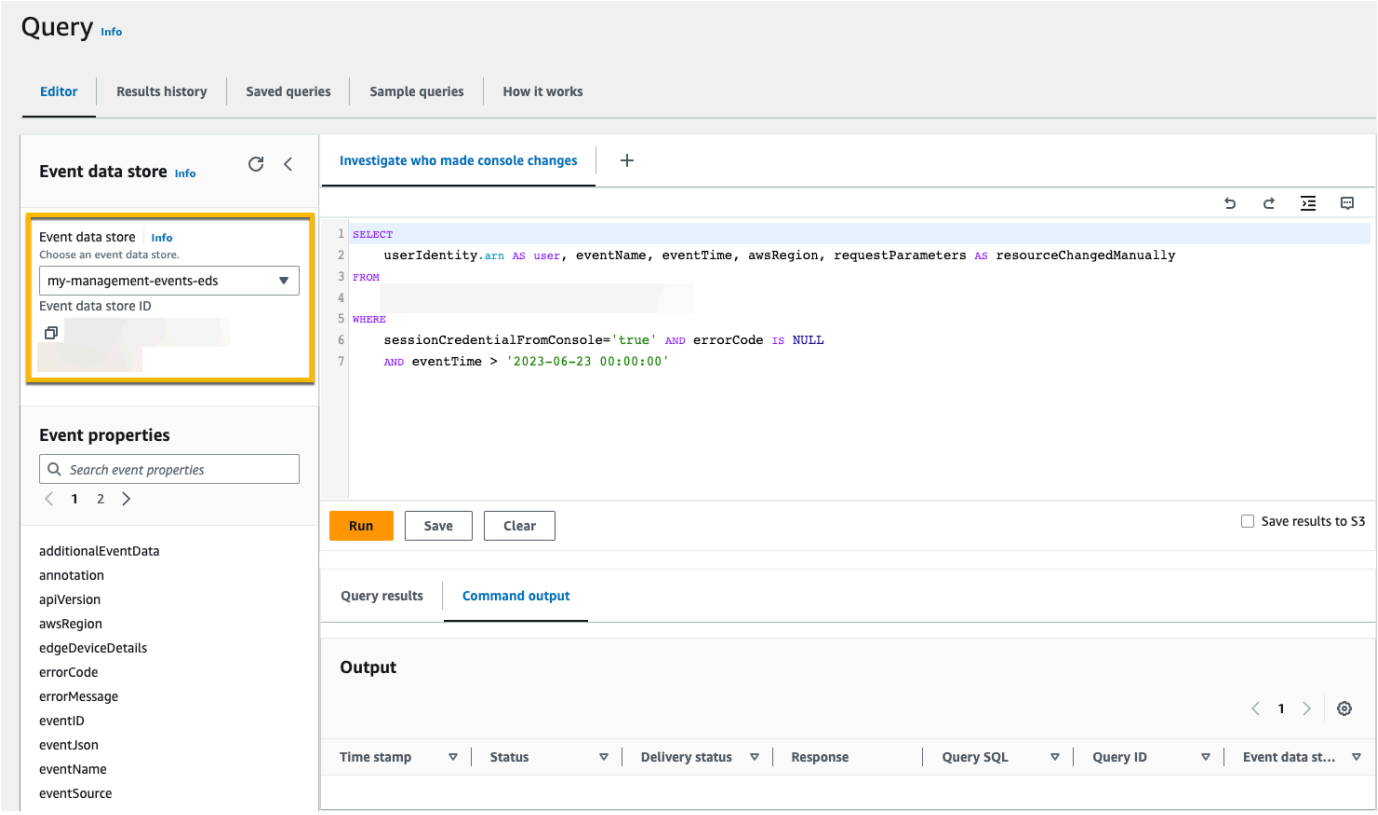
CloudTrail les requêtes sont facturées en fonction de la quantité de données numérisées. Pour aider à contrôler les coûts, nous vous recommandons de limiter les requêtes en ajoutant des horodatages `eventTime` de début et de fin aux requêtes. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Pour afficher et exécuter un exemple de requête

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Requête.
3. Sur la page Requête, sélectionnez l'onglet Exemples de requêtes.
4. Choisissez un exemple de requête dans la liste ou recherchez la requête pour filtrer la liste. Dans cet exemple, nous allons ouvrir la requête Investigate who made console changes en choisissant le Nom de la requête. Cela ouvre la requête dans l'onglet Éditeur.

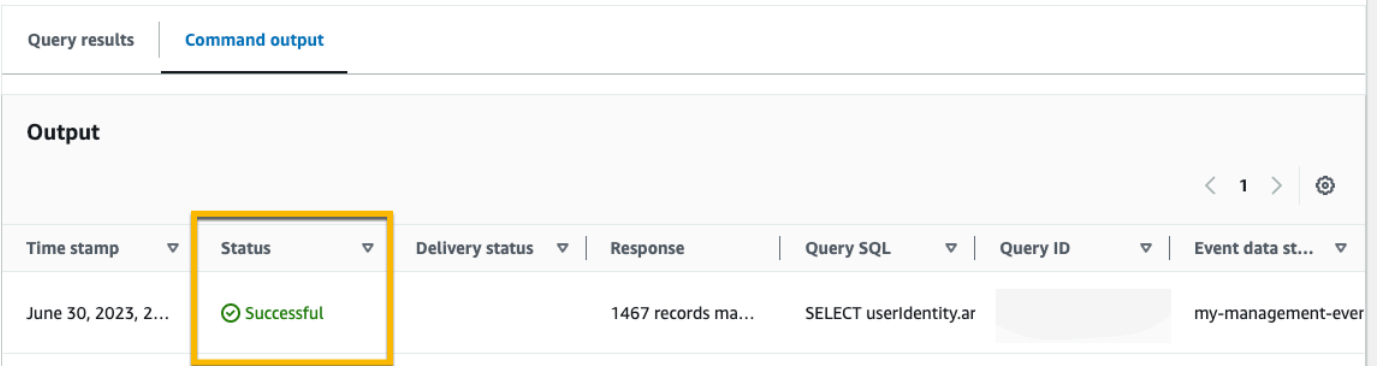


5. Dans l'onglet Éditeur, choisissez l'entrepôt de données d'événement pour lequel vous souhaitez exécuter la requête. Lorsque vous choisissez le magasin de données d'événements dans la liste, l'ID du magasin de données d'événements est CloudTrail automatiquement renseigné dans la `FROM` ligne de l'éditeur de requêtes.

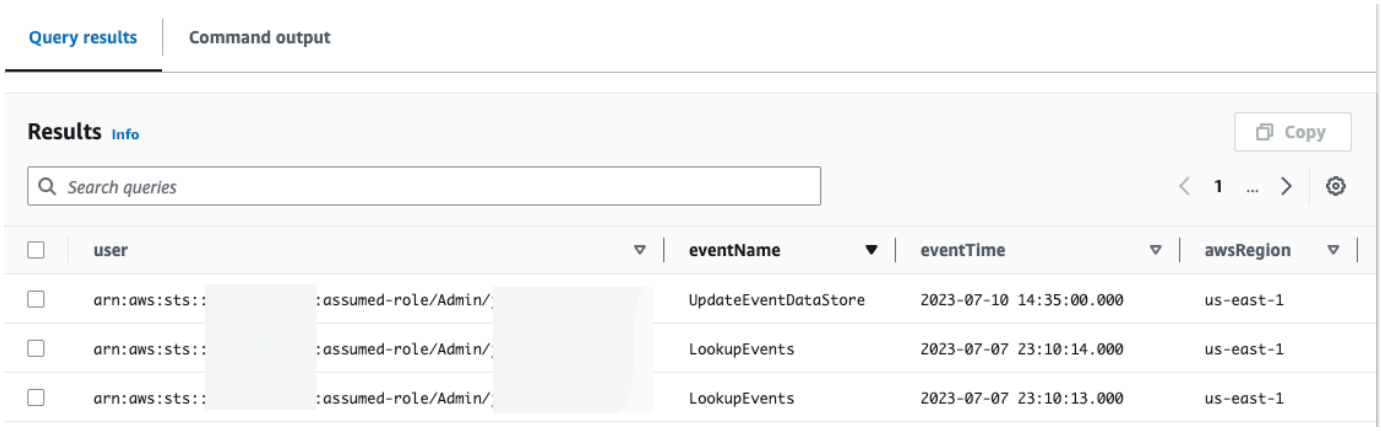


6. Choisissez Exécuter pour exécuter la requête.

   L'onglet Sortie de commande affiche les métadonnées relatives à votre requête, telles que le succès de la requête, le nombre d'enregistrements correspondants et la durée d'exécution de la requête.



   L'onglet Résultats de la requête affiche les données d'événements de l'entrepôt de données d'événement sélectionné qui correspondent à votre requête.



Pour plus d'informations sur l'édition d'une requête, veuillez consulter Créer ou modifier une requête. Pour plus d'informations sur l'exécution d'une requête et l'enregistrement des résultats, veuillez consulter Exécuter une requête et enregistrer les résultats.

Enregistrer les résultats de la requête CloudTrail Lake dans un compartiment S3

Cette procédure pas à pas montre comment enregistrer les résultats des requêtes CloudTrail Lake dans un compartiment S3, puis les télécharger.

Lorsque vous exécutez des requêtes dans CloudTrail Lake, des frais sont facturés en fonction de la quantité de données numérisées par la requête. Aucun frais CloudTrail Lake supplémentaire n'est facturé pour l'enregistrement des résultats des requêtes dans un compartiment S3, mais des frais de stockage S3 sont facturés. Pour de plus amples informations sur la tarification S3, veuillez consulter Tarification Amazon S3.

Lorsque vous enregistrez des résultats de requête, ils peuvent s'afficher dans la CloudTrail console avant d'être visibles dans le compartiment S3, car ils sont fournis CloudTrail une fois l'analyse des requêtes terminée. Bien que la plupart des requêtes soient traitées en quelques minutes, selon la taille de votre banque de données d'événements, la transmission des résultats des requêtes CloudTrail à votre compartiment S3 peut prendre beaucoup plus de temps. CloudTrail fournit les résultats de la requête au compartiment S3 au format gzip compressé. En moyenne, une fois l'analyse de la requête terminée, vous pouvez vous attendre à une latence de 60 à 90 secondes pour chaque Go de données envoyé vers le compartiment S3.

Pour enregistrer les résultats d'une requête dans un compartiment Amazon S3

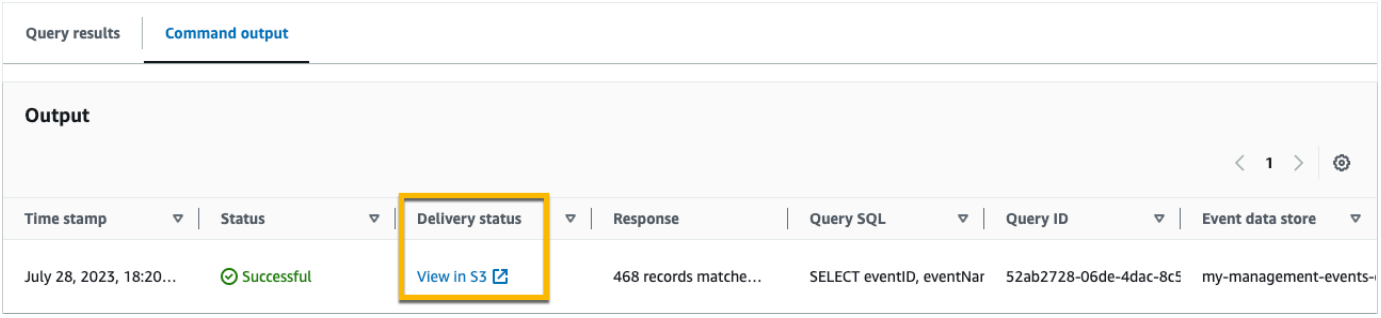
1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Requête.
3. Dans les onglets Requêtes enregistrées ou Exemples de requêtes, choisissez une requête à exécuter en choisissant la valeur dans la colonne SQL de la requête. Dans cet exemple, nous allons choisir l'exemple de requête intitulé Investigate user actions.
4. Dans l'onglet Éditeur, pour Magasin de données d'événement, choisissez un magasin de données d'événement dans la liste déroulante. Lorsque vous choisissez le magasin de données d'événements dans la liste, l'ID du magasin de données d'événements est CloudTrail automatiquement renseigné dans la `From` ligne.
5. Dans cet exemple de requête, nous allons modifier la valeur `userIdentity.`ARN pour spécifier un utilisateur nommé `Admin`, et nous allons conserver les valeurs par défaut pour `eventTime`. Lorsque vous exécutez une requête, la quantité de données analysées vous est facturée. Pour aider à contrôler les coûts, nous vous recommandons de limiter les requêtes en ajoutant des horodatages `eventTime` de début et de fin aux requêtes.

6. Choisissez Enregistrer les résultats dans S3 pour enregistrer les résultats de la requête dans un compartiment S3. Lorsque vous choisissez le compartiment S3 par défaut, il CloudTrail crée et applique les politiques de compartiment requises. Si vous choisissez le compartiment S3 par défaut, votre politique IAM doit inclure une autorisation pour l'`s3:PutEncryptionConfiguration`action, car le chiffrement côté serveur est activé par défaut pour le compartiment. Pour plus d'informations sur l'enregistrement des résultats d'une requête, consultez Informations supplémentaires sur les résultats enregistrés d'une requête. Dans cet exemple, nous utiliserons le compartiment S3 par défaut.

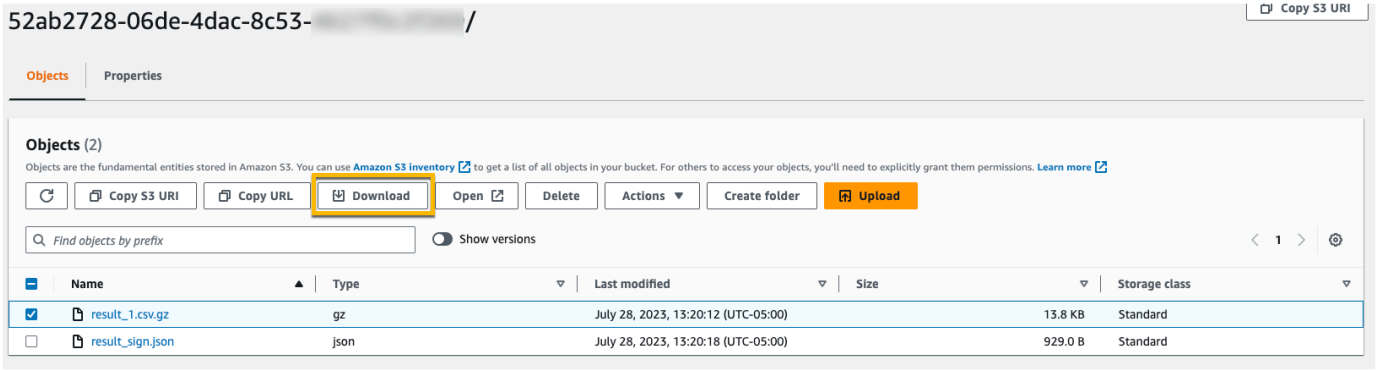
> **Note**
>
> Pour utiliser un compartiment différent, indiquez un nom de compartiment ou choisissez Parcourir S3 pour sélectionner un compartiment. La politique du compartiment doit accorder CloudTrail l'autorisation de fournir les résultats de la requête au compartiment. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake.

7. Cliquez sur Exécuter. Selon la taille de votre magasin de données d'événement et le nombre de jours de données qu'il inclut, l'exécution d'une requête peut prendre plusieurs minutes. L'onglet Command output (Sortie de la commande) affiche l'état d'une requête, et indique si l'exécution d'une requête est terminée. Lorsque l'exécution d'une requête est terminée, ouvrez l'onglet Résultats des requêtes pour afficher un tableau des résultats de la requête active (la requête actuellement affichée dans l'éditeur).
8. Lorsque la livraison des résultats de requête enregistrés à votre compartiment S3 est CloudTrail terminée, la colonne État de livraison fournit un lien vers le compartiment S3 qui contient vos fichiers de résultats de requête enregistrés ainsi qu'un fichier de signature que vous pouvez utiliser pour vérifier les résultats de vos requêtes enregistrés. Choisissez Afficher dans S3 pour afficher les fichiers de résultats de la requête et les fichiers de signature dans le compartiment S3.

> **Note**
>
> Lorsque vous enregistrez des résultats de requête, ils peuvent s'afficher dans la CloudTrail console avant d'être visibles dans le compartiment S3, car ils sont fournis CloudTrail une fois l'analyse des requêtes terminée. Bien que la plupart des requêtes soient traitées en quelques minutes, selon la taille de votre banque de données d'événements, la transmission des résultats des requêtes CloudTrail à votre compartiment S3 peut prendre beaucoup plus de temps. CloudTrail fournit les résultats de la requête au compartiment S3 au format gzip compressé. En moyenne, une fois l'analyse de la requête terminée, vous pouvez vous attendre à une latence de 60 à 90 secondes pour chaque Go de données envoyé vers le compartiment S3.



9. Pour télécharger les résultats de votre requête, choisissez le fichier de résultats de la requête (en l'occurrence `result_1.csv.gz`), puis choisissez Télécharger.



Pour plus d'informations sur la validation des résultats enregistrés d'une requête, veuillez consulter [Validation des résultats enregistrés d'une requête](#).

Consultez vos CloudTrail coûts et votre utilisation avec AWS Cost Explorer

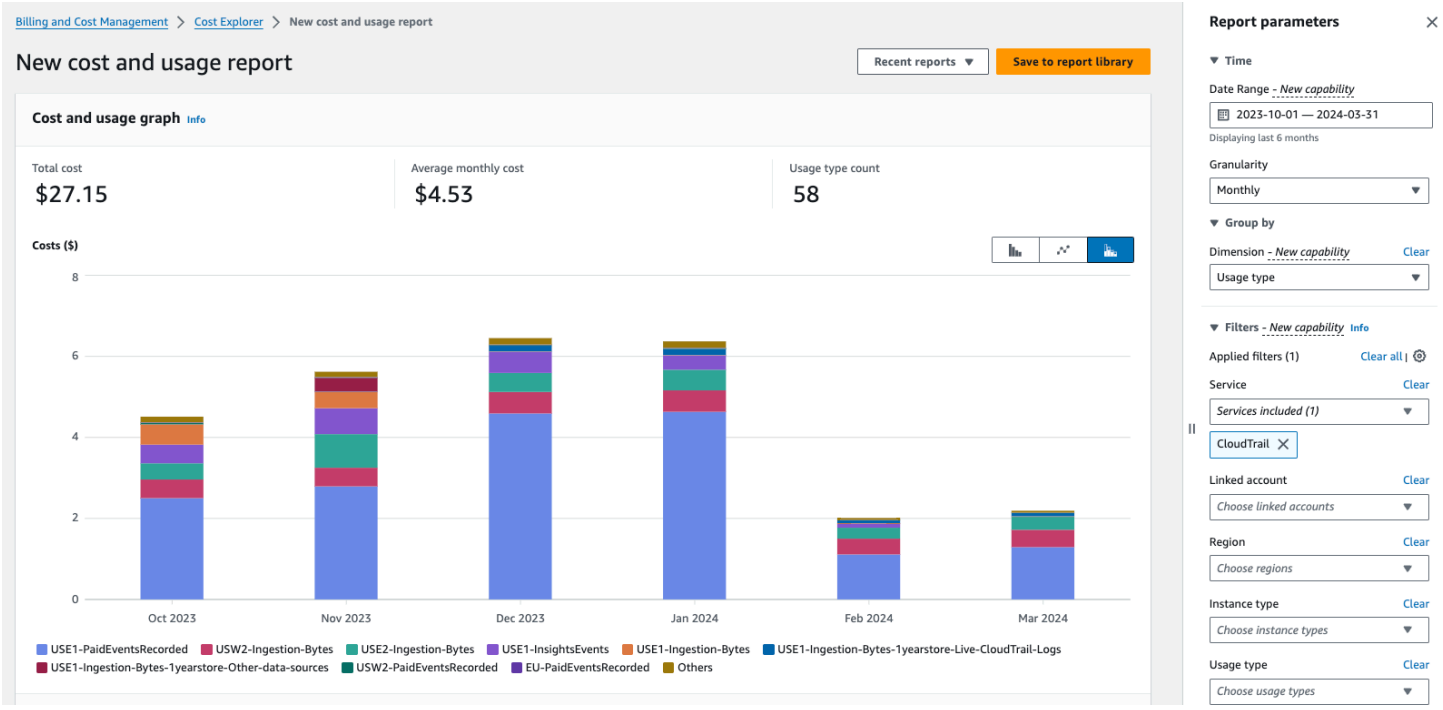
Cette section décrit comment vous pouvez consulter vos CloudTrail coûts et votre utilisation à l'aide de AWS Cost Explorer. Cost Explorer vous permet de visualiser, de comprendre et de gérer vos AWS coûts et votre utilisation au fil du temps.

Pour plus de détails sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Pour afficher les CloudTrail coûts et l'utilisation avec Cost Explorer

1. Connectez-vous à la console Cost Explorer AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cost-management/home#/custom.
2. Sous Heure, choisissez la plage de dates que vous souhaitez analyser.
3. Sous Regrouper par, pour Dimension, choisissez Type d'utilisation.
4. Sous Filtres, pour Service, sélectionnez CloudTrail.

L'image suivante montre un exemple de rapport de coûts filtré CloudTrail et groupé par type d'utilisation.



Passez en revue le type d'utilisation pour voir quelles CloudTrail fonctionnalités ont généré le plus de coûts. Chaque type d'utilisation commence par le code du Région AWS lieu où les frais ont été engagés.

Le tableau suivant décrit les types CloudTrail d'utilisation pour chaque CloudTrail fonctionnalité.

CloudTrail fonctionnalité	Type d'utilisation	Description
CloudTrail sentiers	*region*-FreeEventsRecorded	Le premier exemplaire des événements de gestion remis gratuitement à un Région AWS.
	region-PaidEventsRecorded	Les frais pour les copies supplémentaires des événements de gestion livrées à un Région AWS.
	region-DataEventsRecorded	Les frais de transmission d'événements de données à un Région AWS. Les événements liés aux données entraînent toujours des frais.
CloudTrail lac	*region*-Ingestion-Bytes	Les frais liés à l'ingestion d'événements dans une banque

CloudTrail fonctionnalité	Type d'utilisation	Description
		de données sur les événements de CloudTrail Lake à l'aide de l'option de tarification de rétention sur sept ans. Le prix d'ingestion est basé sur le volume de données ingérées et est le même pour tous les types d'événements.
	region-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	Les frais d'ingestion d'événements de CloudTrail données et d'événements de gestion dans un magasin de données d'événements CloudTrail Lake à l'aide de l'option de tarification de rétention extensible d'un an.

CloudTrail fonctionnalité	Type d'utilisation	Description
	region-Ingestion-Bytes-1yearstore-Other-data-sources	Les frais d'ingestion d'autres sources d'événements dans un magasin de données d'événements CloudTrail Lake à l'aide de l'option de tarification de rétention extensible d'un an. Cela inclut les événements CloudTrail Insights, les éléments de configuration provenant de S3 AWS Config, les preuves provenant AWS Audit Manager, les CloudTrail journaux historiques (non compressés) importés depuis S3 et les événements extérieurs à S3. AWS

CloudTrail fonctionnalité	Type d'utilisation	Description
	region-QueryScanned-Bytes	Les frais d'exécution des requêtes CloudTrail Lake. Lorsque vous exécutez des requêtes dans CloudTrail Lake, des frais sont facturés en fonction de la quantité de données optimisées et compressées numérisées.
CloudTrail Perspectives	*region*-InsightsEvents	Les frais liés aux événements CloudTrail Insights. Pour les événements Insights, vous devez payer des frais basés sur le nombre d'événements de gestion analysés par type d'Insight.

Ressources supplémentaires

- AWS CloudTrail Tarification

- Gestion des coûts des CloudTrail sentiers
- Gestion des coûts CloudTrail du lac

Utilisation de l'historique des CloudTrail événements

CloudTrail est activé par défaut pour votre AWS compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'Historique des événements fournit un enregistrement consultable, interrogeable, téléchargeable et immuable des 90 derniers jours des événements de gestion d'une Région AWS. Ces événements capturent l'activité réalisée par AWS Management Console le biais AWS Command Line Interface des AWS SDK et des API. L'historique des événements enregistre les événements à l' Région AWS endroit où l'événement s'est produit. La consultation de CloudTrail l'historique des événements est gratuite.

Vous pouvez rechercher des événements liés à la création, à la modification ou à la suppression de ressources (tels que des utilisateurs IAM ou des instances Amazon EC2) dans Compte AWS votre région sur la console en consultant CloudTrail la page Historique des événements. Vous pouvez également rechercher ces événements en exécutant la commande aws cloudtrail lookup-events ou en utilisant l'API `LookupEvents`.

Vous pouvez utiliser la page Historique des événements de la CloudTrail console pour afficher, rechercher, télécharger, archiver, analyser et répondre à l'activité du compte dans l'ensemble de votre AWS infrastructure. Vous pouvez personnaliser l'affichage de l'Historique des événements dans la console en sélectionnant le nombre d'événements à afficher sur chaque page et les colonnes à afficher ou à cacher. Vous pouvez également comparer les détails des événements dans l'historique des événements side-by-side. Vous pouvez rechercher des événements par programmation à l'aide des AWS SDK ou. AWS Command Line Interface

> **Note**
>
> Au fil du temps, Services AWS cela pourrait ajouter des événements supplémentaires. CloudTrail enregistre ces événements dans l'historique des événements, mais un enregistrement complet de 90 jours d'activité incluant des événements ajoutés ne sera disponible que 90 jours après l'ajout des événements.
> L'Historique des événements est distinct de tous les journaux de suivi ou entrepôts de données d'événement que vous créez pour votre compte. Les modifications que vous apportez aux entrepôts de données d'événement ou aux journaux de suivi n'ont aucune incidence sur l'Historique des événements.

Les sections suivantes décrivent comment rechercher les événements de gestion récents à l'aide de la CloudTrail console et du AWS CLI, et décrivent comment télécharger un fichier d'événements. Pour plus d'informations sur l'utilisation de l'`LookupEvents`API pour récupérer des informations à partir d' CloudTrail événements, consultez LookupEventsla référence de l'AWS CloudTrail API.

Rubriques

Limites de l'historique des événements

Les limites suivantes s'appliquent à l'Historique des événements.

- La page Historique des événements de la CloudTrail console affiche uniquement les événements de gestion. Elle n'affiche pas les événements liés aux données ni les événements Insights.
- L'Historique des événements est limité aux événements des 90 derniers jours. Pour un enregistrement continu des événements de votre site Compte AWS, créez un magasin de données d'événements ou un suivi.
- Lorsque vous téléchargez des événements depuis la page Historique des événements de la CloudTrail console, vous pouvez télécharger jusqu'à 200 000 événements dans un seul fichier. Si vous atteignez la limite de 200 000 événements, la CloudTrail console vous proposera la possibilité de télécharger des fichiers supplémentaires.
- L'historique des événements ne fournit pas d'agrégation d'événements au niveau de l'organisation. Pour enregistrer les événements au sein de votre organisation, créez un entrepôt de données d'événement ou un journal de suivi d'organisation.
- Une recherche dans l'historique des événements est limitée à un seul Compte AWS, ne renvoie que les événements d'un seul Région AWSévénement et ne peut pas interroger plusieurs attributs. Vous ne pouvez appliquer qu'un seul filtre d'attributs et un filtre de plage de temps.

  Vous pouvez créer un magasin de données d'événements CloudTrail Lake pour effectuer des requêtes sur plusieurs attributs et Régions AWS. Vous pouvez également effectuer des requêtes sur plusieurs Comptes AWS au sein d'une AWS Organizations organisation. Dans CloudTrail Lake, vous pouvez interroger plusieurs types d'événements, notamment des événements de gestion, des événements de données, des événements Insights, des éléments de AWS Config configuration,

des preuves d'Audit Manager et AWS des non-événements. CloudTrail Les requêtes Lake offrent une vue plus approfondie et plus personnalisable des événements que de simples recherches de clés et de valeurs dans l'historique des événements ou en cours d'exécution`LookupEvents`. Pour plus d'informations, consultez Travailler avec AWS CloudTrail Lake et Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

- Vous ne pouvez pas exclure AWS KMS les événements de l'API Amazon RDS Data de l'historique des événements ; les paramètres que vous appliquez à un magasin de données de suivi ou d'événement ne s'appliquent pas à l'historique des événements.

Afficher les événements de gestion récents à l'aide de la console

Vous pouvez utiliser la page Historique des événements de la CloudTrail console pour consulter les 90 derniers jours d'événements de gestion dans un Région AWS. Vous pouvez également télécharger un fichier avec ces informations, ou un sous-ensemble des informations en fonction du filtre et de la plage de temps que vous choisissez. Vous pouvez personnaliser votre affichage de l'Historique des événements en sélectionnant le nombre d'événements à afficher sur chaque page et en choisissant les colonnes à afficher dans la console. Vous pouvez également rechercher et filtrer des événements par les types de ressources disponibles pour un service particulier. Vous pouvez sélectionner jusqu'à cinq événements dans l'historique des événements et comparer leurs détails side-by-side.

Historique des événements n'affiche pas les événements de données. Pour afficher les événements liés aux données, créez un entrepôt de données d'événement ou un journal de suivi.

Après 90 jours, les événements ne sont plus affichés dans Historique des événements. Vous ne pouvez pas supprimer manuellement des événements de l'historique des événements.

Pour en savoir plus sur les spécificités de la CloudTrail journalisation des événements pour un service spécifique, consultez la documentation relative à ce service. Pour plus d'informations, consultez AWS sujets de service pour CloudTrail.

> **Note**
>
> Pour un enregistrement continu de l'activité et des événements survenus au cours des 90 derniers jours, créez un magasin de données sur les événements ou un suivi.

Pour consulter l'Historique des événements

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, choisissez Event history (Historique des événements). Vous voyez une liste filtrée des événements, avec les événements les plus récents affichés d'abord. Le filtre par défaut pour les événements est Lecture seule, défini sur false. Il est possible d'effacer ce filtre en choisissant X à droite du filtre.
3. Vous pouvez filtrer les événements en fonction d'un seul attribut, que vous pouvez sélectionner dans la liste déroulante. Pour filtrer un attribut, choisissez-le dans la liste déroulante et entrez la valeur complète de l'attribut. Par exemple, pour afficher tous les événements de connexion à la console, choisissez le filtre Nom de l'événement, puis spécifiez ConsoleLogin. Ou, pour afficher les derniers événements de gestion S3, choisissez le filtre de source d'événements et spécifiez`s3.amazonaws.com`.
4. Pour consulter un événement de gestion spécifique, choisissez le nom de l'événement. Sur la page des détails de l'événement, vous pouvez consulter les détails de l'événement, les ressources référencées et l'enregistrement de l'événement.
5. Pour comparer des événements, sélectionnez jusqu'à cinq événements en remplissant leurs cases à cocher dans la marge gauche de la table Historique des événements. Vous pouvez consulter les détails des événements sélectionnés side-by-side dans le tableau Comparer les détails des événements.
6. Vous pouvez enregistrer l'historique des événements en le téléchargeant en tant que fichier au format JSON ou CSV. Le téléchargement de l'historique de votre événement peut prendre quelques minutes.

Table des matières

Naviguer entre les pages

Vous pouvez naviguer entre les pages de l'Historique des événements en choisissant la page que vous souhaitez consulter. Vous pouvez également consulter la page suivante et la page précédente dans l'Historique des événements.

Choisissez < pour afficher la page précédente de l'Historique des événements.

Choisissez < pour afficher la page suivante de l'Historique des événements.

Personnaliser l'affichage

Vous pouvez personnaliser l'affichage de l'historique des événements dans la CloudTrail console en sélectionnant l'une des préférences suivantes.

- Taille de page : choisissez si vous souhaitez afficher 10, 25 ou 50 événements sur chaque page.
- Renvoyer le texte à la ligne : renvoyer le texte à la ligne pour que vous puissiez voir tout le texte de chaque événement.
- Lignes rayées : ombragez une ligne sur deux du tableau.
- Affichage de l'heure de l'événement : choisissez d'afficher l'heure de l'événement en UTC ou dans le fuseau horaire local.
- Sélectionner les colonnes visibles : sélectionnez les colonnes à afficher. Par défaut, les colonnes suivantes sont affichées :
  - Nom de l'événement
  - Heure de l'événement
  - Nom utilisateur
  - Source de l'événement
  - Type de ressource
  - Nom de la ressource

> **Note**
>
> Vous ne pouvez pas modifier l'ordre des colonnes, ni supprimer manuellement les événements dans l'historique des événements.

Pour personnaliser l'affichage

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sélectionnez Historique des événements.
3. Choisissez l'icône d'engrenage.
4. Pour Taille de page, choisissez le nombre d'événements à afficher sur une page.
5. Choisissez Renvoyer le texte à la ligne pour voir tout le texte de chaque événement.
6. Choisissez Lignes rayées pour ombrager une ligne sur deux du tableau.
7. Pour l'Affichage de l'heure de l'événement, choisissez d'afficher l'heure de l'événement en UTC ou dans le fuseau horaire local. UTC est sélectionné par défaut.
8. Dans Sélectionnez les colonnes visibles, sélectionnez les colonnes que vous souhaitez afficher. Fermez les colonnes que vous ne souhaitez pas afficher.
9. Lorsque vous avez terminé vos modifications, sélectionnez Confirmer.

Filtrage CloudTrail des événements

Par défaut, l'historique des événements utilise un filtre d'attributs pour exclure de l'affichage les événements en lecture seule. Ce filtre d'attributs est nommé Lecture seule et est défini sur faux. Vous pouvez supprimer ce filtre pour afficher les événements de lecture et d'écriture. Si vous souhaitez n'afficher que les événements de Lecture, vous pouvez modifier la valeur du filtre sur vrai. Vous pouvez également filtrer les événements selon d'autres attributs. Vous pouvez en outre filtrer par plage de temps.

> **Note**
>
> Vous ne pouvez appliquer qu'un seul filtre d'attributs et un filtre de plage de temps. Vous ne pouvez pas appliquer plusieurs filtres d'attributs.

AWS clé d'accès

ID de clé d' AWS accès utilisé pour signer la demande. Si la demande a été faite avec des informations d'identification de sécurité temporaires, il s'agit de l'ID de clé d'accès des informations d'identification temporaires.

ID de l'événement

L' CloudTrail ID de l'événement. Chaque événement présente un ID unique.

Nom de l'événement

Nom de l'événement. Par exemple, vous pouvez filtrer en fonction d'événements IAM comme `CreatePolicy`, ou d'événements Amazon EC2; comme `RunInstances`.

Source de l'événement

Le AWS service auquel la demande a été adressée, tel que `iam.amazonaws.com` ou`s3.amazonaws.com`. Vous pouvez faire défiler la liste des sources d'événements après avoir choisi le filtre Source de l'événement.

Lecture seule

Type de lecture de l'événement. Les événements sont classés comme événements de lecture ou d'écriture. Si cet attribut est défini sur faux, les événements de lecture ne sont pas inclus dans la liste des événements affichés. Par défaut, ce filtre d'attributs est appliqué et la valeur est définie sur faux.

Nom de la ressource

Le nom ou l'ID de la ressource référencée par l'événement. Par exemple, le nom de la ressource peut être « auto-scaling-test-group » pour un groupe Auto Scaling ou « i-12345678910 » pour une instance EC2.

Type de ressource

Le type de la ressource référencée par l'événement. Par exemple, un type de ressource peut être `Instance` pour EC2 ou `DBInstance` pour RDS. Les types de ressources varient pour chaque AWS service.

Plage horaire

La plage horaire dans laquelle vous voulez filtrer les événements. Vous avez le choix entre une Plage relative ou une Plage absolue. Vous pouvez filtrer les événements des 90 derniers jours.

Nom utilisateur

L'identité référencée par l'événement. Par exemple, il peut s'agir d'un utilisateur, d'un nom de rôle ou d'une fonction du service.

Si aucun événement n'est journalisé pour l'attribut ou l'heure que vous avez choisi, la liste des résultats est vide. Vous pouvez appliquer un seul filtre d'attributs, en plus de la plage de temps. Si vous choisissez un autre filtre d'attribut, la plage de temps que vous avez spécifiée est conservée.

Les étapes suivantes expliquent comment filtrer sur les attributs.

Pour filtrer par attribut

1. Pour filtrer les résultats selon un attribut, choisissez un attribut dans la liste déroulante Attributs de recherche, puis tapez ou choisissez une valeur pour l'attribut dans la zone de texte.
2. Pour supprimer un filtre d'attributs, cliquez sur le X à droite de la zone de filtre d'attributs.

Les étapes suivantes expliquent comment filtrer sur une date et une heure de début et de fin.

Pour filtrer selon une date et une heure de début et de fin

1. Pour restreindre la plage de temps pour les événements que vous voulez voir, sélectionnez une plage de temps dans la barre réservée à la plage de temps. Vous avez le choix entre une Plage relative ou une Plage absolue.

   Choisissez Plage relative pour sélectionner une valeur prédéfinie ou choisir une plage personnalisée. Les valeurs prédéfinies sont de 30 minutes, 1 heure, 12 heures ou 1 jour. Pour spécifier une plage de temps personnalisée, choisissez Personnaliser.

   Choisissez Plage absolue pour spécifier une heure de début et de fin spécifique. Vous pouvez également choisir entre le fuseau horaire local et l'heure UTC.
2. Pour supprimer un filtre de plage de temps, choisissez Effacer et rejeter dans la barre réservée à la plage de temps.

Afficher les détails d'un événement

1. Sélectionnez un événement dans la liste des résultats pour en afficher les détails.
2. Les ressources référencées dans l'événement sont affichées dans la table Ressources référencées sur la page de détails de l'événement.
3. Certaines ressources référencées ont des liens. Cliquez sur le lien pour ouvrir la console pour cette ressource.

4. Faites défiler jusqu'à Enregistrement d'événement sur la page de détails pour voir l'enregistrement d'événement JSON, également appelé événement charge utile.
5. Choisissez Historique des événements dans la piste de navigation de la page pour fermer la page de détails de l'événement et revenir à Historique des événements.

Téléchargement des événements

Vous pouvez télécharger l'historique des événements enregistrés en tant que fichier au format JSON ou CSV. Vous pouvez télécharger jusqu'à 200 000 événements dans un seul fichier. Si vous atteignez la limite de 200 000 événements, la CloudTrail console vous permettra de télécharger des fichiers supplémentaires. Utilisez des filtres et des plages de temps pour réduire la taille du fichier que vous téléchargez.

> **Note**
>
> CloudTrail les fichiers d'historique des événements sont des fichiers de données qui contiennent des informations (telles que les noms des ressources) qui peuvent être configurées par des utilisateurs individuels. Certaines données peuvent éventuellement être interprétées comme des commandes dans des programmes utilisés pour lire et analyser ces données (injection CSV). Par exemple, lorsque CloudTrail des événements sont exportés au format CSV et importés dans un tableur, ce programme peut vous avertir de problèmes de sécurité. Vous devez choisir de désactiver ce contenu afin de garantir la sécurité de votre système. Désactivez toujours les liens ou les macros provenant des fichiers d'historique des événements téléchargés.

1. Ajouter un filtre et une plage de temps pour les événements dans Historique des événements que vous souhaitez télécharger. Par exemple, vous pouvez spécifier le nom d'événement, `StartInstances`, et indiquer une plage de temps pour les trois derniers jours d'activité.
2. Choisissez Téléchargez les événements, puis Télécharger au format CSV ou Télécharger au format JSON. Le téléchargement commence immédiatement.

   > **Note**
   >
   > Le téléchargement peut prendre un certain temps. Pour des résultats plus rapides, utilisez un filtre spécifique ou une plage de temps plus courte pour affiner les résultats avant de commencer le processus de téléchargement. Il est possible d'annuler un

téléchargement. Si vous annulez un téléchargement, un téléchargement partiel incluant uniquement certaines données d'événement peut se trouver sur votre ordinateur local. Pour télécharger l'historique complet des événements, relancez le téléchargement.

3. Une fois le téléchargement terminé, ouvrez le fichier pour afficher les événements que vous avez spécifiés.
4. Pour annuler votre téléchargement, choisissez Annuler, puis confirmez en choisissant Annuler le téléchargement. Si vous devez relancer un téléchargement, attendez que l'annulation du téléchargement précédent soit terminée.

Affichage des ressources référencées avec AWS Config

AWS Config enregistre les détails de configuration, les relations et les modifications apportées à vos AWS ressources.

Dans le volet Ressources référencées, choisissez la colonne « dans la chronologie AWS Config des ressources » pour afficher la ressource dans la AWS Config console.

Si l'icône est grise, si elle AWS Config n'est pas activée ou si elle n'enregistre pas le type de ressource. Cliquez sur l'icône pour accéder à la AWS Config console afin d'activer le service ou de commencer à enregistrer ce type de ressource. Pour plus d'informations, voir Configuration à AWS Config l'aide de la console dans le guide du AWS Config développeur.

Si Lien non disponible apparaît dans la colonne, la ressource ne peut pas être consultée pour l'une des raisons suivantes :

- AWS Config ne prend pas en charge le type de ressource. Pour plus d'informations, consultez Ressources, éléments de configuration et relations pris en charge dans le AWS Config Guide du développeur.
- AWS Config la prise en charge du type de ressource a récemment été ajoutée, mais elle n'est pas encore disponible sur la CloudTrail console. Vous pouvez rechercher la ressource dans la AWS Config console pour voir la chronologie de la ressource.
- La ressource appartient à une autre personne Compte AWS.
- La ressource appartient à une autre personne Service AWS, telle qu'une politique IAM gérée.

- La ressource a été créée puis immédiatement supprimée.
- La ressource a été créée ou mise à jour récemment.

Pour accorder aux utilisateurs l'autorisation en lecture seule d'afficher les ressources dans la AWS Config console, consultez. Octroi de l'autorisation AWS Config d'afficher les informations sur la CloudTrail console

Pour plus d'informations à ce sujet AWS Config, consultez le guide du AWS Config développeur.

Afficher les événements de gestion récents à l'aide du AWS CLI

Vous pouvez consulter les événements CloudTrail de gestion des 90 derniers jours pour le moment à l' Région AWS aide de la aws cloudtrail lookup-events commande. La aws cloudtrail lookup-events commande affiche les événements Région AWS là où ils se sont produits.

La recherche prend en charge les attributs suivants pour les événements de gestion :

- AWS clé d'accès
- ID de l'événement
- Nom de l'événement
- Source de l'événement
- Lecture seule
- Nom de la ressource
- Type de ressource
- Nom utilisateur

Tous les autres attributs sont facultatifs.

La commande `lookup-events` contient les options suivantes :

- `--max-items <integer>` : nombre total d'éléments à renvoyer dans la sortie de la commande. Si le nombre total d'éléments disponibles est supérieur à la valeur spécifiée, un jeton `NextToken` est fourni dans la sortie de la commande. Pour reprendre la pagination, fournissez la valeur de `NextToken` dans l'argument starting-token d'une commande suivante. N'utilisez pas l'élément de réponse `NextToken` directement en dehors de l' AWS CLI.

- `--start-time` *`<timestamp>`* : spécifie que seuls les événements qui se produisent au moment indiqué ou après sont renvoyés. Si l'heure de début spécifiée survient après l'heure de fin spécifiée, une erreur est renvoyée.
- `--lookup-attributes` <integer> : contient une liste d'attributs de recherche. Actuellement, la liste ne peut contenir qu'un seul élément.
- `--generate-cli-skeleton` <string> : imprime un squelette JSON sur une sortie standard sans envoyer de demande d'API. S'il est fourni sans valeur ou sans valeur, imprime un exemple d'entrée JSON qui peut être utilisé comme argument pour `--cli-input-json`. De même, si une entrée yaml est fournie, elle imprimera un exemple d'entrée YAML pouvant être utilisé avec `--cli-input-yaml`. Si la valeur en sortie est fournie, elle valide les entrées de commande et renvoie un exemple de sortie JSON pour cette commande. Le squelette JSON généré n'est pas stable entre les versions du AWS CLI et il n'existe aucune garantie de rétrocompatibilité dans le squelette JSON généré.
- `--cli-input-json` <string> : lit les arguments à partir de la chaîne JSON fournie. La chaîne JSON suit le format fourni par le paramètre `--generate-cli-skeleton`. Si d'autres arguments sont fournis sur la ligne de commande, ces valeurs remplaceront les valeurs fournies par JSON. Il n'est pas possible de transmettre des valeurs binaires arbitraires en utilisant une valeur fournie par JSON, car la chaîne sera interprétée littéralement. Cela ne peut pas être spécifié en même temps que le paramètre `--cli-input-yaml`.

Pour obtenir des informations générales sur l'utilisation de l'interface de ligne de AWS commande, consultez le guide de AWS Command Line Interface l'utilisateur.

Table des matières

Prérequis

- Pour exécuter AWS CLI des commandes, vous devez installer le AWS CLI. Pour plus d'informations, voir Commencer avec le AWS CLI.
- Assurez-vous que votre AWS CLI version est supérieure à 1.6.6. Pour vérifier la version de la CLI, exécutez aws --version sur la ligne de commande.
- Pour définir le compte et Région AWS le format de sortie par défaut pour une AWS CLI session, utilisez la aws configure commande. Pour plus d'informations, voir Configuration de l'interface de ligne de AWS commande.

> **Note**
>
> Les CloudTrail AWS CLI commandes distinguent les majuscules et minuscules.

Obtenir de l'aide de la ligne de commande

Pour voir l'aide de la ligne de commande pour `lookup-events`, tapez la commande suivante :

```
aws cloudtrail lookup-events help
```

Recherche d'événements

> **Important**
>
> Le taux de demandes de recherche est limité à deux par seconde, par compte et par région. Si cette limite est dépassée, une erreur de régulation se produit.

Pour voir les dix derniers événements, tapez la commande suivante :

```
aws cloudtrail lookup-events --max-items 10
```

Un événement renvoyé ressemble à l'exemple fictif suivant, qui a été mis en forme pour faciliter la lecture :

```
{
```

```
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
                  \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                  \"eventType\":\"AwsApiCall\",
                  \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```


Pour une explication des champs liés à la recherche dans la sortie, consultez la section Champs de résultat de la recherche ultérieurement dans ce document. Pour une explication des champs de l' CloudTrail événement, voirCloudTrail enregistrer le contenu.

Spécifier le nombre d'événements à renvoyer

Pour spécifier le nombre d'événements à renvoyer, tapez la commande suivante :

```
aws cloudtrail lookup-events --max-items <integer>
```

Les valeurs possibles vont de 1 à 50. L'exemple suivant renvoie un événement.

```
aws cloudtrail lookup-events --max-items 1
```

Recherche d'événements par plage de temps

Les événements survenus au cours des 90 derniers jours sont disponibles pour la recherche. Pour spécifier une plage de temps, tapez la commande suivante :

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *<timestamp>* spécifie, in UTC, que seuls les événements qui se produisent au moment indiqué ou après sont renvoyés. Si l'heure de début spécifiée survient après l'heure de fin spécifiée, une erreur est renvoyée.

`--end-time` *<timestamp>* spécifie, en UTC, que seuls les événements qui se produisent au moment indiqué ou avant sont renvoyés. Si l'heure de fin spécifiée survient avant l'heure de début spécifiée, une erreur est renvoyée.

L'heure de début par défaut est la première date à laquelle les données sont disponibles au cours des 90 derniers jours. L'heure de fin par défaut est l'heure de l'événement qui s'est produit le plus près de l'heure actuelle.

Tous les horodatages sont affichés en UTC.

Recherche d'événements par attribut

Pour filtrer selon un attribut, tapez la commande suivante :

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Vous ne pouvez spécifier qu'une seule paire clé-valeur d'attribut pour chaque commande lookup-events. Les valeurs suivantes sont valides pour `AttributeKey`. Les noms de valeur sont sensibles à la casse.

- AccessKeyId
- EventId
- EventName
- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

La longueur maximale du AttributeValue est de 2 000 caractères. Les caractères suivants (« _ », « », « , », « \\n ») comptent pour deux caractères dans la limite de 2000 caractères.

Exemples de recherche d'attribut

L'exemple de commande suivant renvoie les événements dans lesquels la valeur de AccessKeyId est AKIAIOSFODNN7EXAMPLE.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

L'exemple de commande suivant renvoie l'événement pour le paramètre spécifié CloudTrailEventId.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

L'exemple de commande suivant renvoie les événements dans lesquels la valeur de EventName est RunInstances.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

L'exemple de commande suivant renvoie les événements dans lesquels la valeur de EventSource est iam.amazonaws.com.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

L'exemple de commande suivant renvoie des événements d'écriture. Elle exclut les événements de lecteur, tels que `GetBucketLocation` et `DescribeStream`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

L'exemple de commande suivant renvoie les événements dans lesquels la valeur de `ResourceName` est `CloudTrail_CloudWatchLogs_Role`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

L'exemple de commande suivant renvoie les événements dans lesquels la valeur de `ResourceType` est `AWS::S3::Bucket`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

L'exemple de commande suivant renvoie les événements dans lesquels la valeur de `Username` est `root`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Spécifier la page de résultats suivante

Pour obtenir la page de résultats suivante à partir d'une commande `lookup-events`, tapez la commande suivante :

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

où la valeur de *<token>* provient du premier champ de la sortie de la commande précédente.

Lorsque vous utilisez `--next-token` dans une commande, vous devez utiliser les mêmes paramètres que dans la commande précédente. Par exemple, supposons que vous exécutiez la commande suivante :

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Pour obtenir la page de résultats suivante, votre commande suivante se présente comme suit :

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

Extraction de l'entrée JSON d'un fichier

AWS CLI Pour certains AWS services, `--generate-cli-skeleton` deux paramètres peuvent être utilisés pour générer un modèle JSON que vous pouvez modifier et utiliser comme entrée pour le `--cli-input-json` paramètre. `--cli-input-json` Cette section décrit comment utiliser ces paramètres avec `aws cloudtrail lookup-events`. Pour des informations plus générales, voir AWS CLI squelettes et fichiers d'entrée.

Pour rechercher CloudTrail des événements en obtenant une entrée JSON à partir d'un fichier

1. Créer un modèle d'entrée à utiliser avec `lookup-events` en redirigeant la sortie de `--generate-cli-skeleton` vers un fichier, comme dans l'exemple suivant.

   ```
   aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
   ```

   Le fichier modèle généré (dans ce cas, LookupEvents .txt) ressemble à ceci :

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
           }
       ],
       "StartTime": null,
       "EndTime": null,
       "MaxResults": 0,
       "NextToken": ""
   }
   ```

2. Utilisez un éditeur de texte pour modifier le code JSON le cas échéant. L'entrée JSON doit contenir uniquement des valeurs qui sont spécifiées.

> **Important**
>
> Toutes les valeurs vides ou null doivent être supprimées du modèle pour que vous puissiez l'utiliser.

L'exemple suivant spécifie un intervalle de temps et un nombre maximal de résultats à retourner.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Pour utiliser le fichier modifié comme entrée, utilisez la syntaxe `--cli-input-json file://<nom de fichier>`, comme dans l'exemple suivant :

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> Vous pouvez utiliser d'autres arguments sur la même ligne de commande en tant que `--cli-input-json`.

Champs de résultat de la recherche

Evénements

Liste des événements de recherche basée sur l'attribut de recherche et la plage de temps qui ont été spécifiés. La liste des événements est triée par heure, le dernier événement arrivant en tête. Chaque entrée contient des informations sur la demande de recherche et inclut une représentation sous forme de chaîne de l' CloudTrail événement récupéré.

Les entrées suivantes décrivent les champs dans chaque événement de recherche.

CloudTrailEvent

Chaîne JSON qui contient une représentation d'objet de l'événement renvoyé. Pour plus d'informations sur chacun des éléments renvoyés, consultez Contenu du corps d'un enregistrement.

EventId

Chaîne qui contient le GUID de l'événement retourné.

EventName

Chaîne qui contient le nom de l'événement renvoyé.

EventSource

Le AWS service auquel la demande a été adressée.

EventTime

Date et heure, au format de temps UNIX, de l'événement.

Ressources

Liste de ressources référencées par l'événement qui a été renvoyé. Chaque entrée de ressource spécifie un type de ressource et un nom de ressource.

ResourceName

Chaîne qui contient le nom de la ressource référencée par l'événement.

ResourceType

Chaîne qui contient le type d'une ressource référencée par l'événement. Lorsque le type de ressource ne peut pas être déterminé, la valeur null est renvoyée.

Username

Chaîne qui contient le nom d'utilisateur du compte pour l'événement renvoyé.

NextToken

Chaîne pour obtenir la page de résultats suivante d'une commande `lookup-events` précédente. Pour utiliser le jeton, les paramètres doivent être identiques à ceux de la commande d'origine. Si aucune entrée `NextToken` n'apparaît dans la sortie, cela signifie qu'il n'y a aucun résultat à renvoyer.

Travailler avec AWS CloudTrail Lake

AWS CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement, qui sont des ensembles inaltérables d'événements basés sur des critères que vous sélectionnez en appliquant les sélecteurs d'événements avancés. Vous pouvez conserver les données d'événement dans une banque de données d'événement jusqu'à 3 653 jours (environ 10 ans) si vous choisissez l'option de tarification de rétention extensible d'un an, ou jusqu'à 2 557 jours (environ 7 ans) si vous choisissez l'option de tarification de rétention de sept ans. Les sélecteurs que vous appliquez à une banque de données d'événements contrôlent les événements qui persistent et que vous pouvez interroger. CloudTrail Lake est une solution d'audit qui peut compléter votre système de conformité et vous aider à résoudre les problèmes en temps quasi réel.

CloudTrail Stockages de données sur les événements du lac

Lorsque vous créez un magasin de données d'événement, vous choisissez le type d'événements à inclure dans celui-ci. Vous pouvez créer un magasin de données d'événements pour inclure CloudTrail des événements, CloudTrail des événements Insights, des éléments de AWS Config configuration, des AWS Audit Manager preuves ou des événements extérieurs à AWS. Chaque banque de données d'événements ne peut contenir qu'une catégorie d'événements spécifique (par exemple, des éléments de AWS Config configuration), car le schéma d'événement est unique à la catégorie d'événements. Vous pouvez stocker les événements d'une organisation AWS Organizations dans un magasin de données d'événements d'organisation, y compris les événements provenant de plusieurs régions et comptes. Vous pouvez exécuter des requêtes SQL sur plusieurs magasins de données d'événement en utilisant les mots-clés SQL JOIN pris en charge. Pour plus d'informations sur l'exécution de requêtes sur plusieurs magasins de données d'événement, consultez Prise en charge avancée des requêtes multitables.

Vous pouvez copier les événements du parcours dans un magasin de données d'événements nouveau ou existant pour créer un point-in-time instantané des événements enregistrés dans le parcours. Pour plus d'informations, consultez Copier des événements de journal de suivi dans un magasin de données d'événement.

Vous pouvez fédérer un magasin de données d'événement pour voir les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et exécuter des

requêtes SQL sur les données d'événement à l'aide d'Amazon Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés par CloudTrail. Lorsque vous configurez un magasin de données d'événements, vous pouvez choisir d'utiliser votre propre AWS Key Management Service clé. L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

Vous pouvez contrôler l'accès aux actions sur les magasins de données d'événement à l'aide de l'autorisation basée sur des balises. Pour plus d'informations et d'exemples, consultez aussi Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications dans ce guide.

Vous pouvez utiliser les tableaux de bord CloudTrail Lake pour visualiser les données de vos magasins de données d'événements. Chaque tableau de bord est composé de plusieurs widgets et chaque widget représente une requête SQL. Pour de plus amples informations sur le tableau de bord Lake, veuillez consulter Afficher les tableaux de bord de CloudTrail Lake.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

CloudTrail Lake prend en charge CloudWatch les métriques Amazon, qui fournissent des informations sur les données ingérées et les octets de stockage. Pour plus d'informations sur les CloudWatch métriques prises en charge, consultez CloudWatch Métriques prises en charge.

> **Note**
>
> CloudTrail fournit généralement des événements dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti.

CloudTrail Intégrations de lacs

Vous pouvez utiliser les intégrations CloudTrail Lake pour enregistrer et stocker les données d'activité des utilisateurs provenant de l'extérieur AWS, de n'importe quelle source dans vos environnements hybrides, telles que des applications internes ou SaaS hébergées sur site ou dans le cloud, des machines virtuelles ou des conteneurs. Après avoir créé des magasins de données d'événements dans CloudTrail Lake et créé un canal pour enregistrer les événements d'activité, vous appelez l'`PutAuditEvents`API pour y intégrer CloudTrail l'activité de votre application. Vous pouvez ensuite utiliser CloudTrail Lake pour rechercher, interroger et analyser les données enregistrées par vos applications.

Les intégrations peuvent également enregistrer des événements dans vos magasins de données d'événements provenant de plus d'une douzaine de CloudTrail partenaires. Dans le cadre d'une intégration de partenaires, vous créez des stockages de données d'événement de destination, un canal et une politique de ressources. Après avoir créé l'intégration, vous fournissez l'ARN du canal au partenaire. Il existe deux types d'intégrations : directe et solution. Dans le cas des intégrations directes, le partenaire appelle l'`PutAuditEvents`API pour transmettre les événements au magasin de données d'événements de votre AWS compte. Avec les intégrations de solutions, l'application s'exécute dans votre AWS compte et l'application appelle l'`PutAuditEvents`API pour transmettre les événements au magasin de données d'événements de votre AWS compte.

Pour plus d'informations sur les intégrations, voir Créer une intégration avec une source d'événements extérieure à. AWS

CloudTrail Requêtes sur le lac

CloudTrail Les requêtes Lake offrent une vue plus approfondie et plus personnalisable des événements que de simples recherches de clés et de valeurs dans l'historique des événements ou en cours d'exécution`LookupEvents`. Une recherche dans l'historique des événements est limitée à un seul Compte AWS, ne renvoie que les événements d'un seul Région AWSévénement et ne peut pas interroger plusieurs attributs. En revanche, les utilisateurs de CloudTrail Lake peuvent exécuter des requêtes SQL complexes sur plusieurs champs d'événements. CloudTrail Lake prend en charge toutes les `SELECT` instructions et fonctions Presto valides. Pour plus d'informations sur les fonctions et opérateurs SQL pris en charge, veuillez consulter Functions and Operators sur le site Web de documentation de Presto.

Vous pouvez enregistrer les requêtes CloudTrail Lake pour une utilisation future et consulter les résultats des requêtes pendant sept jours au maximum. Lorsque vous exécutez des requêtes, vous pouvez enregistrer leurs résultats dans un compartiment Amazon S3.

La CloudTrail console fournit un certain nombre d'exemples de requêtes qui peuvent vous aider à commencer à écrire vos propres requêtes. Pour plus d'informations, consultez Afficher des exemples de requêtes dans la CloudTrail console.

CloudTrail Les requêtes relatives au lac entraînent des frais. Lorsque vous exécutez des requêtes dans Lake, vous payez en fonction de la quantité de données analysées. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Ressources supplémentaires

Les ressources suivantes peuvent vous aider à mieux comprendre ce qu'est CloudTrail Lake et comment vous pouvez l'utiliser.

- Modernisez la gestion de vos journaux d'audit à l'aide de CloudTrail Lake (YouTube vidéo)
- Enregistrer les événements d'activité non liés àAWS des sources dans AWS CloudTrail le lac (YouTube vidéo)
- Analysez les journaux d'activité avec AWS CloudTrail Lake et Amazon Athena (vidéo) YouTube
- Obtenez de la visibilité dans les journaux d'activité de votre personnel et de l'identité de vos clients (AWS blog)
- Utilisation de AWS CloudTrail Lake pour identifier les anciennes connexions TLS aux points de terminaison AWS du service (blog)AWS
- Comment Arctic Wolf utilise AWS CloudTrail Lake pour simplifier la sécurité et les opérations (AWS blog)
- CloudTrail FAQ sur le lac
- AWS CloudTrail API Reference
- AWS CloudTrail Référence de l'API de données
- AWS CloudTrail Guide d'intégration des partenaires

CloudTrail Régions soutenues par les lacs

CloudTrail Lake est actuellement pris en charge dans les domaines suivants Régions AWS :

Nom de la région	Région
US East (Virginie du Nord)	us-east-1
USA Est (Ohio)	us-east-2
USA Ouest (Californie du Nord)	us-west-1
US West (Oregon)	us-west-2
Afrique (Le Cap)	af-south-1
Asie-Pacifique (Hong Kong)	ap-east-1
Asie-Pacifique (Hyderabad)	ap-south-2
Asie-Pacifique (Jakarta)	ap-southeast-3
Asie-Pacifique (Mumbai)	ap-south-1
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Singapour)	ap-southeast-1
Asie-Pacifique (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europe (Francfort)	eu-central-1
Europe (Irlande)	eu-west-1
Europe (Londres)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3

Nom de la région	Région
Europe (Espagne)	eu-south-2
Europe (Stockholm)	eu-north-1
Europe (Zurich)	eu-central-2
Israël (Tel Aviv)	il-central-1
Moyen-Orient (Bahreïn)	me-south-1
Moyen-Orient (EAU)	me-central-1
Amérique du Sud (São Paulo)	sa-east-1
AWS GovCloud (USA Est)	us-gov-east-1
AWS GovCloud (US-Ouest)	us-gov-west-1

Pour plus d'informations sur les points CloudTrail de terminaison de service, consultez la section AWS CloudTrail Points de terminaison et quotas.

Pour plus d'informations sur l'utilisation CloudTrail dans le AWS GovCloud (US) Regions, consultez la section Points de terminaison du service dans le guide de l'AWS GovCloud (US) utilisateur.

CloudTrail Concepts et terminologie relatifs aux lacs

Cette section décrit les principaux concepts et termes qui vous aideront à utiliser AWS CloudTrail Lake.

Concepts et terminologie

- Magasins de données d'événement
- Intégrations
- Requêtes
- Tableau de bord

Magasins de données d'événement

Les événements sont agrégés dans des magasins de données d'événement, qui sont des ensembles inaltérables d'événements basés sur des critères que vous sélectionnez en appliquant les sélecteurs d'événements avancés.

Vous pouvez créer un magasin de données d'événements pour enregistrer les événements CloudTrail de gestion et les événements de données, les événements CloudTrail Insights, les AWS Audit Manager preuves, les éléments de AWS Config configuration ou les événements extérieurs à AWS.

Sélecteurs d'événements avancés

Les sélecteurs d'événements avancés déterminent les événements à inclure dans un magasin de données d'événement. Ils vous aident à contrôler les coûts en ne journalisant que les événements qui sont importants pour vous.

Pour les événements de gestion et les événements de données, vous pouvez utiliser des sélecteurs d'événements avancés pour filtrer les événements. Par exemple, si vous créez un magasin de données d'événements pour collecter des événements de gestion, vous pouvez filtrer les événements de l'API de données Amazon Relational Database Service AWS Key Management Service (Amazon RDS AWS KMS) ou les exclure (). Généralement, AWS KMS les actions telles que `EncryptDecrypt`, et `GenerateDataKey` génèrent plus de 99 % des événements.

Pour les éléments de AWS Config configuration, les preuves d'Audit Manager ou les événements extérieurs aux sélecteurs d' AWSévénements avancés ne sont utilisés que pour inclure des événements de ce type dans le magasin de données d'événements.

Fédération

Fédération vous permet de consulter les métadonnées associées à un magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événements à l'aide d'Amazon Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger.

Lorsque vous activez la fédération de requêtes Lake, CloudTrail crée les ressources fédérées en votre nom et enregistre ces ressources auprès AWS Lake Formationde. Une fois la fédération de Lake activée, vous pouvez directement interroger les données de votre événement dans Athena

sans avoir à effectuer d'étapes supplémentaires. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

Option de tarification

Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la tarification, consultez Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

Période de conservation

La période de conservation d'un magasin de données d'événements détermine la durée pendant laquelle les données d'événements sont conservées dans le magasin de données d'événements. CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

Période de conservation par défaut

La période de conservation par défaut d'un magasin de données d'événement est le nombre de jours par défaut pendant lesquels les données d'événements sont conservées dans le magasin de données d'événement. Pendant la période de conservation par défaut d'un magasin de données d'événement, le stockage est inclus dans le prix d'ingestion sans frais supplémentaires. Après la période de conservation par défaut, le prix du stockage est fixé à pay-as-you-go.

Période de conservation maximale

La période de conservation maximale d'un magasin de données d'événement représente le nombre maximal de jours pendant lesquels vous pouvez conserver les données dans un magasin de données d'événement.

Protection de la résiliation

Par défaut, les magasins de données d'événement activent la protection contre la résiliation, qui protège un magasin de données d'événement contre toute suppression accidentelle. Pour supprimer un magasin de données d'événement avec la protection de résiliation activée, choisissez Modifier la protection contre la résiliation dans le menu Actions de la page de détails du magasin de données d'événement. Vous pouvez ensuite supprimer le magasin de données

d'événement. Pour plus d'informations, consultez Modifier la protection contre le licenciement à l'aide de la console.

Intégrations

Vous pouvez utiliser les intégrations de CloudTrail Lake pour enregistrer et stocker les données d'activité des utilisateurs provenant des sources suivantes :

- À l'extérieur de AWS
- Vous pouvez journaliser et stocker les données d'activité des utilisateurs provenant des sources que vous souhaitez dans vos environnements hybrides, telles que des applications internes ou SaaS (logiciel en tant que service) hébergées sur site ou dans le cloud, des machines virtuelles ou des conteneurs

Une intégration nécessite un canal pour diffuser les événements et un magasin de données d'événement pour recevoir les événements. Après avoir configuré votre intégration, appelez l'opération PutAuditEventsAPI pour intégrer CloudTrail l'activité de votre application. Vous pouvez ensuite utiliser CloudTrail Lake pour rechercher, interroger et analyser les données enregistrées par vos applications. Pour plus d'informations, consultez Créez une intégration avec une source d'événements en dehors de AWS.

Type d'intégration

Il existe deux types d'intégrations : directe et solution. Avec les intégrations directes, le partenaire appelle l'API `PutAuditEvents` pour transmettre les événements au magasin de données d'événement pour votre Compte AWS. Dans le cas des intégrations de solutions, l'application s'exécute dans votre environnement Compte AWS et l'application appelle l'opération `PutAuditEvents` API pour transmettre les événements au magasin de données d'événements qui vous Compte AWS concerne.

Canaux

Organisez des événements provenant de sources extérieures au AWS travail en utilisant des canaux pour diffuser dans CloudTrail Lake des événements provenant de partenaires externes qui travaillent avec CloudTrail vous ou provenant de vos propres sources. Lorsque vous créez un canal, vous sélectionnez un ou plusieurs magasins de données d'événement pour stocker les événements provenant de la source du canal. Vous pouvez modifier les magasins de données d'événement de destination d'un canal selon vos besoins, à condition qu'ils soient configurés pour

journaliser les événements `eventCategory="ActivityAuditLog"`. Lorsque vous créez un canal pour les événements d'un partenaire externe, vous fournissez un Amazon Resource Name (ARN) de canal au partenaire ou à l'application source.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. La politique basée sur les ressources attachée au canal permet à la source de transmettre des événements via celui-ci. Si un canal ne dispose d'aucune politique de ressources, seul le propriétaire du canal peut appeler l'API `PutAuditEvents` sur celui-ci. Pour plus d'informations, consultez AWS CloudTrail exemples de politiques basées sur les ressources.

Requêtes

Les requêtes dans CloudTrail Lake sont créées en SQL. Vous pouvez créer une requête dans l'onglet CloudTrail Lake Editor en écrivant la requête en SQL à partir de zéro, ou en ouvrant une requête enregistrée ou un exemple de requête et en la modifiant. Vous ne pouvez pas remplacer un exemple de requête inclus par vos modifications, mais vous pouvez l'enregistrer en tant que nouvelle requête. Pour plus d'informations, consultez Créer ou modifier une requête.

CloudTrail Lake prend en charge toutes les Presto `SELECT` déclarations et fonctions valides. Pour plus d'informations sur les fonctions et opérateurs SQL pris en charge, veuillez consulter Fonctions et opérateurs sur le site Web de documentation de Presto.

Tableau de bord

En utilisant le tableau de bord CloudTrail Lake, vous pouvez visualiser les événements dans un magasin de données d'événements et voir les tendances des événements, telles que le top Services AWS, les utilisateurs et les erreurs. Pour plus d'informations, consultez Afficher les tableaux de bord de CloudTrail Lake.

Type de tableau de bord

Les types de tableaux de bord disponibles pour un magasin de données d'événement dépendent de la configuration des sélecteurs d'événements avancés du magasin de données d'événement. Par exemple, si un type de tableau de bord affiche des informations sur les événements de CloudTrail gestion, vous ne pouvez sélectionner le tableau de bord que si le magasin de données d'événements actuellement sélectionné collecte CloudTrail des événements de gestion.

Les types de tableaux de bord disponibles sont les suivants :

- Tableau de bord d'ensemble — Affiche les utilisateurs les plus actifs Régions AWS, et Services AWS par nombre d'événements. Vous pouvez également consulter des informations sur l'activité des événements de gestion `read` et `write`, les événements les plus limités et les principales erreurs. Ce tableau de bord est disponible pour les magasins de données d'événement qui collectent des événements de gestion.
- Tableau de bord Événements de gestion : affiche les événements de connexion à la console, les événements de refus d'accès, les actions destructrices et les principales erreurs par utilisateur. Vous pouvez également consulter des informations sur les versions TLS et les appels TLS obsolètes par utilisateur. Ce tableau de bord est disponible pour les entrepôts de données d'événement qui collectent des événements de gestion.
- Tableau de bord Événements de données S3 : affiche l'activité du compte Amazon S3, les objets S3 les plus consultés, les principaux utilisateurs S3 et les principales actions S3. Ce tableau de bord est disponible pour les magasins de données d'événement qui collectent des événements de données Amazon S3.
- Tableau de bord Événements Insights : affiche la proportion globale d'événements Insights par type Insights, la proportion d'événements Insights par type Insights pour les principaux utilisateurs et services, et le nombre d'événements Insights par jour. Le tableau de bord inclut également un widget qui répertorie jusqu'à 30 jours d'événements Insights. Ce tableau de bord n'est disponible que pour les entrepôts de données d'événement qui collectent des événements Insights.

> **Note**
>
> - Une fois que vous avez activé CloudTrail Insights pour la première fois dans le magasin de données d'événements source, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée. Pour plus d'informations, consultez Comprendre la diffusion d'événements Insights.
> - Le tableau de bord Événements Insights n'affiche que les informations relatives aux événements Insights collectés par l'entrepôt de données d'événement sélectionné, qui sont déterminées par la configuration de l'entrepôt de données d'événement source. Par exemple, si vous configurez le magasin de données d'événement source pour activer les événements Insights sur `ApiCallRateInsight`, mais pas sur `ApiErrorRateInsight`, vous ne verrez aucune information sur les événements Insights sur `ApiErrorRateInsight`.

Widgets

Les widgets sont les composants qui constituent un tableau de bord et fournissent une visualisation, telle qu'un graphique linéaire ou un graphique à barres. Chaque widget représente une requête sous-jacente. Lorsque vous choisissez Exécuter des requêtes, CloudTrail exécute une requête générée par le système pour renseigner les données de chaque widget.

CloudTrail Stockages de données sur les événements du lac

Les événements sont agrégés dans des magasins de données d'événement, qui sont des ensembles inaltérables d'événements basés sur des critères que vous sélectionnez en appliquant les sélecteurs d'événements avancés.

Lorsque vous créez un magasin de données d'événements dans CloudTrail Lake, vous choisissez le type d'événements à inclure dans votre magasin de données d'événements. Vous pouvez créer un magasin de données d'événements pour inclure CloudTrail des données ou des événements de gestion, CloudTrail des événements Insights, des éléments de AWS Config configuration ou des événements extérieurs à AWS. Chaque type de banque de données d'événements ne peut contenir que des catégories d'événements spécifiques (par exemple, des éléments de AWS Config configuration), car le schéma d'événement est unique à la catégorie d'événements. Vous pouvez exécuter des requêtes SQL sur plusieurs magasins de données d'événement en utilisant les mots-clés SQL JOIN pris en charge. Pour plus d'informations sur l'exécution de requêtes sur plusieurs magasins de données d'événement, consultez Prise en charge avancée des requêtes multitables.

Le tableau suivant montre les catégories d'événement prises en charge pour chaque type d'entrepôt de données d'événement. La colonne eventCategory indique la valeur que vous devez spécifier dans les sélecteurs d'événements avancés pour collecter les événements de ce type.

Type d'événement (console)	eventCategory (API)	Description

CloudTrail événements	`Management`
	
	`Data`
		Ce type de magasin de données d'événements peut collecter CloudTrail des événements de gestion et de données. Pour plus d'informations, voir Création d'un magasin de données d'CloudTrail événements pour les événements.

Type d'événement (console)	eventCategory (API)	Description
CloudTrail Événements Insights	`Insight`	Ce type de banque de données d'événements peut collecter CloudTrail des événements Insights. Pour recevoir des événements Insights, vous avez besoin d'un magasin de données d'événements source qui enregistre les événements CloudTrail de gestion et active Insights. Pour plus d'informations sur la création des magasins de données d'événements source et de destination, voir Création d'un magasin de données d'événements pour les événements CloudTrail Insights.
Éléments de configuration	`ConfigurationItem`	Ce type de magasin de données d'événements peut collecter des éléments AWS Config de configuration. Pour plus d'informations, voir Création d'un magasin de données d'événements pour les éléments AWS Config de configuration.
Événements issus de l'intégration	`ActivityAuditLog`	Ce type de magasin de données d'événements peut collecter des AWS événements non liés aux intégrations. Pour plus d'informations, voir Création d'un magasin de données d'événements pour les événements extérieurs à AWS.

Vous pouvez également créer un magasin de données d'événements à titre de AWS Audit Manager preuve à l'aide de la console Audit Manager. Pour plus d'informations sur l'agrégation des preuves dans CloudTrail Lake à l'aide d'Audit Manager, voir Comprendre le fonctionnement de l'outil de recherche de preuves avec CloudTrail Lake dans le guide de AWS Audit Manager l'utilisateur.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le

magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Les sections suivantes décrivent comment créer, mettre à jour et gérer des banques de données d'événements.

Rubriques

Création, mise à jour et gestion de banques de données d'événements à l'aide de la console

Vous pouvez utiliser la CloudTrail console pour créer, mettre à jour et gérer vos magasins de données d'événements. Vous pouvez également démarrer et arrêter l'ingestion d'événements sur un magasin de données d'événements et activer la fédération de requêtes Lake à l'aide de la console.

L'utilisation de la CloudTrail console pour créer ou mettre à jour des banques de données d'événements présente les avantages suivants :

- Si c'est la première fois que vous créez un magasin de données d'événements, la CloudTrail console vous permet de visualiser les fonctionnalités et options disponibles.
- Si vous configurez un magasin de données d'événements pour enregistrer les événements de données, la CloudTrail console vous permet de visualiser les types de données disponibles. Pour plus d'informations, consultez Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console et Journalisation des événements de données.
- Si vous configurez un magasin de données d'événements pour enregistrer des événements en dehors de AWS, l'utilisation de la CloudTrail console vous permet de consulter les informations sur les partenaires disponibles. Pour plus d'informations, consultez Création d'un magasin de données d'événements pour les événements extérieurs AWS à la console.

Rubriques

- Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console
- Créez un magasin de données d'événements pour les événements CloudTrail Insights à l'aide de la console
- Créez un magasin de données d'événements pour les éléments AWS Config de configuration à l'aide de la console
- Création d'un magasin de données d'événements pour les événements extérieurs AWS à la console
- Mettre à jour un magasin de données d'événements avec la console
- Arrêter et démarrer l'ingestion d'événements avec la console
- Modifier la protection contre le licenciement à l'aide de la console
- Supprimer un magasin de données d'événements à l'aide de la console
- Restaurer un magasin de données d'événements à l'aide de la console

Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console

Les banques de données relatives aux CloudTrail événements peuvent enregistrer les événements CloudTrail de gestion et de données. Vous pouvez conserver les données d'événement dans une banque de données d'événement jusqu'à 3 653 jours (environ 10 ans) si vous choisissez l'option de tarification de rétention extensible d'un an, ou jusqu'à 2 557 jours (environ 7 ans) si vous choisissez l'option de tarification de rétention de sept ans.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Pour créer un magasin de données d'événements pour la CloudTrail gestion ou les événements de données

Utilisez cette procédure pour créer un magasin de données d'événements qui enregistre les événements de CloudTrail gestion, les événements de données ou à la fois les événements de gestion et les événements de données.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configure event data store (Configurer un magasin de données d'événement), dans General details (Détails généraux), saisissez un nom pour le magasin de données d'événement. Un nom est obligatoire.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
     - Période de conservation par défaut : 366 jours.
     - Période de conservation maximale : 3 653 jours
   - Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
     - Période de conservation par défaut : 2 557 jours.
     - Période de conservation maximale : 2 557 jours
6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez

une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

> **Note**
>
> Si vous copiez des événements de suivi dans cette banque de données d'événements, vous ne CloudTrail copierez aucun événement s'il `eventTime` est antérieur à la période de conservation spécifiée. Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.

7. (Facultatif) Pour activer le chiffrement en utilisant AWS Key Management Service, choisissez Utiliser le mien AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

   L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

   > **Note**
   >
   > Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de

visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.

b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.

c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans la zone Balises, vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre magasin de données d'événement. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section AWS Ressources de balisage dans le Guide de l'utilisateur AWS des ressources de balisage.
10. Choisissez Suivant pour configurer le magasin de données d'événement.
11. Sur la page Choisir des événements, choisissez AWS des événements, puis CloudTraildes événements.
12. Pour les CloudTrail événements, choisissez au moins un type d'événement. Par défaut, Management events (Événements de gestion) est sélectionné. Vous pouvez ajouter à la fois des événements de gestion et de données à votre magasin de données d'événement. Pour plus d'informations sur les événements de gestion, veuillez consulter Journalisation des événements de gestion. Pour plus d'informations sur les événements de données, veuillez consulter Journalisation des événements de données.

13. (Facultatif) Choisissez Copier les événements du journal de suivi si vous voulez copier les événements d'un journal de suivi existant pour exécuter des requêtes sur des événements passés. Pour copier les événements de journal de suivi vers le magasin de données d'événement d'une organisation, vous devez utiliser le compte de gestion de l'organisation. Le compte d'administrateur délégué ne peut pas copier les événements de journal de suivi vers le magasin de données d'événement d'une organisation. Pour plus d'informations et des considérations sur la copie d'événements de journal de suivi, veuillez consulter Considérations pour copier les événements de journal de suivi.
14. Pour que votre magasin de données d'événement collecte les événements de tous les comptes d'une organisation AWS Organizations , sélectionnez Activer pour tous les comptes de mon organisation. Vous devez être connecté au compte de gestion ou au compte administrateur délégué de l'organisation pour créer un magasin de données d'événement qui collecte les événements pour une organisation.

> **Note**
>
> Pour copier des événements de journal de suivi ou activer des événements Insights, vous devez être connecté au compte de gestion de votre organisation.

15. Développez les paramètres supplémentaires pour choisir si vous souhaitez que votre banque de données d'événements collecte les événements pour tous Régions AWS ou uniquement les événements actuels Région AWS, et choisissez si la banque de données d'événements ingère les événements. Par défaut, votre entrepôt de données d'événement collecte les événements de toutes les régions de votre compte et commence à ingérer les événements dès sa création.

    a. Vous pouvez également sélectionner Inclure uniquement la région actuelle dans mon entrepôt de données d'événement pour n'inclure que les événements journalisés dans la région actuelle. Si vous ne choisissez pas cette option, votre magasin de données d'événement inclura des événements de toutes les régions.

    b. Désélectionnez Ingérer des événements si vous ne souhaitez pas que l'entrepôt de données d'événement commence à ingérer des événements. Par exemple, vous souhaiterez peut-être désélectionner Ingérer des événements si vous copiez des événements du journal de suivi et que vous ne souhaitez pas que l'entrepôt de données d'événement inclue des événements futurs. Par défaut, l'entrepôt de données d'événement commence à ingérer les événements dès sa création.

16. Si votre entrepôt de données d'événement inclut des événements de gestion, vous pouvez choisir l'une des options suivantes. Pour plus d'informations sur les événements de gestion, veuillez consulter Journalisation des événements de gestion.

    a. Choisissez si vous souhaitez inclure les événements de Lecture, les événements d'Écriture ou les deux. Au moins une unité est obligatoire.

    b. Choisissez d'exclure AWS Key Management Service ou d'exclure les événements de l'API Amazon RDS Data de votre banque de données d'événements.

    c. Choisissez d'activer ou non Insights. Pour activer Insights, vous devez configurer un entrepôt de données d'événement de destination afin de collecter les événements Insights en fonction de l'activité des événements de gestion dans cet entrepôt de données d'événement.

       Si vous choisissez d'activer Insights, procédez comme suit.

       i. Dans Activer Insights, choisissez le stockage d'événements de destination qui enregistrera les événements Insights. L'entrepôt de données d'événement de destination collectera les événements Insights en fonction de l'activité de gestion des événements dans cet entrepôt de données d'événement. Pour plus d'informations sur la création de l'entrepôt de données événements de destination, veuillez consulter Pour créer un entrepôt de données d'événement de destination qui journalise les événements Insights.

       ii. Choisissez les types Insights. Vous pouvez choisir le Taux d'appels d'API, le Taux d'erreur de l'API ou les deux. Vous devez journaliser les événements de gestion Écriture pour journaliser les événements Insights afin de connaître le Taux d'appels d'API. Vous devez journaliser les événements de gestion Lecture ou Écriture pour journaliser les événements Insights afin de connaître le Taux d'erreur de l'API.

17. Pour inclure des événements de données dans votre magasin de données d'événement, procédez comme suit.

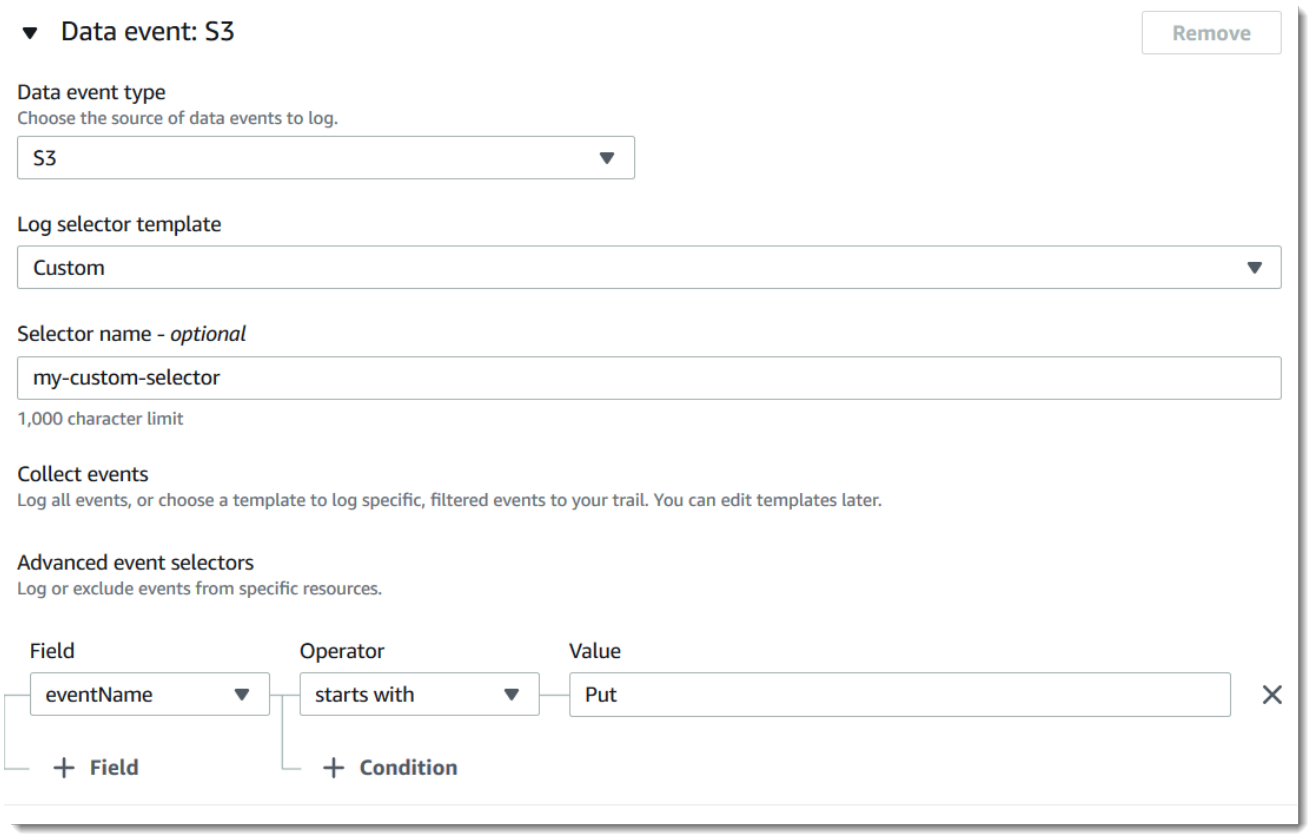
    a. Choisissez un type d'événement de données. Il s'agit de Service AWS la ressource sur laquelle les événements de données sont enregistrés. Pour enregistrer les événements de données pour AWS Glue les tables créées par Lake Formation, choisissez Lake Formation comme type de données.

    b. Dans Modèle de sélecteur de journaux, choisissez un modèle. Vous pouvez choisir de journaliser tous les événements de données, les événements `readOnly`, les événements `writeOnly`, ou Personnaliser pour créer un sélecteur de journaux personnalisé.

c. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.

d. Dans Sélecteurs d'événement avancés, créez des expressions en choisissant des valeurs pour Champ, Opérateur et Valeur. Les sélecteurs d'événement avancés pour un magasin de données d'événement fonctionnent de la même manière que les sélecteurs d'événement avancés que vous appliquez à un journal de suivi. Pour plus d'informations sur la création de sélecteurs d'événements avancés, voir Filtrer les événements de données à l'aide de sélecteurs d'événements avancés.

   L'exemple suivant utilise un modèle de sélecteur de journaux Personnalisé pour choisir uniquement les noms d'événement à partir d'objets S3 qui commencent par `Put`, comme `PutObject`. Étant donné que le sélecteur d'événements avancé n'inclut ni n'exclut aucun autre type d'événement ou ARN de ressource, tous les événements de données S3, en lecture et en écriture, dont le nom commence par `Put`, sont consignés dans l'entrepôt de données d'événement.



> **Important**
>
> Pour exclure ou inclure des événements de données avec des sélecteurs d'événement avancés à l'aide d'un ARN de compartiment S3, utilisez toujours l'opérateur Starts with (Commence par).

e. Vous pouvez également développer Affichage JSON pour afficher vos sélecteurs d'événements avancés sous forme de bloc JSON.

f. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Ajouter un type d'événement de données. Répétez les étapes a à cette étape pour configurer les sélecteurs d'événements avancés pour le type d'événement de données.

18. Pour copier des événements de journal de suivi existant dans votre magasin de données d'événement, procédez comme suit.

    a. Sélectionnez le journal de suivi que vous voulez copier. Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, choisissez Enter S3 URI, puis Browse S3 pour accéder au préfixe. Si le compartiment S3 source pour le suivi utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique en matière de clés KMS autorise CloudTrail le déchiffrement des données. Si votre compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé afin de CloudTrail permettre le déchiffrement des données contenues dans le compartiment. Pour plus d'informations sur la mise à jour de la stratégie de clé KMS, veuillez consulter Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source.

    b. Choisissez la plage horaire pour copier les événements. CloudTrail vérifie le préfixe et le nom du fichier journal pour vérifier que le nom contient une date comprise entre les dates de début et de fin choisies avant de tenter de copier les événements de suivi. Vous avez le choix entre Plage relative ou Plage absolue. Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez une plage de temps antérieure à la création du magasin de données d'événement.

> **Note**
>
> CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Par exemple, si la période de conservation d'un magasin de données d'événements est de 90 jours, aucun événement de suivi datant de `eventTime` plus de 90 jours ne CloudTrail sera copié.

- Si vous choisissez Plage relative, vous pouvez choisir de copier les événements enregistrés au cours des 6 derniers mois, 1 an, 2 ans, 7 ans ou une plage personnalisée. CloudTrail copie les événements enregistrés pendant la période choisie.
- Si vous choisissez la plage absolue, vous pouvez choisir une date de début et une date de fin spécifiques. CloudTrail copie les événements survenus entre les dates de début et de fin choisies.

c. Pour Autorisations, sélectionnez l'une des options de rôle IAM suivantes. Si vous choisissez un rôle IAM existant, vérifiez que la politique de rôle IAM fournit les autorisations nécessaires. Pour plus d'informations sur la mise à jour des autorisations du rôle IAM, consultez Autorisations IAM pour copier les événements de journal de suivi.

- Sélectionnez Créer un nouveau rôle (recommandé) pour créer un nouveau rôle IAM. Pour Enter IAM role name, saisissez le nom du rôle. CloudTrail crée automatiquement les autorisations nécessaires pour ce nouveau rôle.
- Choisissez Utiliser un ARN de rôle IAM personnalisé pour utiliser un rôle IAM personnalisé qui n'est pas répertorié. Pour Enter IAM role ARN (Saisir l'ARN du rôle IAM), saisissez l'ARN IAM.
- Choisissez un rôle IAM existant dans la liste déroulante.

19. Choisissez Suivant pour examiner vos préférences.
20. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
21. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

À partir de ce moment, l'entrepôt de données d'événement capture les événements qui correspondent à ses sélecteurs d'événement avancés (si vous avez gardé l'option Ingérer les événements sélectionnée). Les événements s'étant produits avant la création du magasin de données d'événement ne figurent pas dans celui-ci, à moins que vous ne choisissiez de copier les événements de suivi existants.

Vous pouvez désormais exécuter des requêtes sur votre magasin de données d'événement. L'onglet Samples queries (Exemples de requêtes) fournit des exemples de requêtes pour vous aider à démarrer. Pour plus d'informations sur la création et la modification des requêtes, consultez Créer ou modifier une requête.

Vous pouvez également consulter le tableau de bord CloudTrail Lake pour visualiser les événements dans votre banque de données d'événements. Pour de plus amples informations sur le tableau de bord Lake, veuillez consulter Afficher les tableaux de bord de CloudTrail Lake.

Exemple : création d'un magasin de données d'événements pour la gestion des événements

Cette procédure pas à pas vous explique comment créer un magasin de données d'événements qui enregistre tous les événements de gestion dans toutes les AWS régions et n'enregistre aucun événement de données. Des exemples d'événements de gestion incluent des événements liés à la sécurité, tels que les événements IAM `CreateUser` et `AttachRolePolicy`, les événements de ressource tels que `RunInstances` et `CreateBucket`, et bien plus encore.

Pour créer un magasin de données d'événement pour des événements de gestion

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configurer le magasin de données d'événements, dans Détails généraux, donnez un nom à votre magasin de données d'événements, tel que *`my-management-events-eds`*. Comme bonne pratique, utilisez un nom qui identifie rapidement l'objectif de l'entrepôt de données d'événement. Pour plus d'informations sur les exigences en matière de CloudTrail dénomination, consultezExigences de dénomination.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de

données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

Les options suivantes sont disponibles :

- Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
  - Période de conservation par défaut : 366 jours.
  - Période de conservation maximale : 3 653 jours
- Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
  - Période de conservation par défaut : 2 557 jours.
  - Période de conservation maximale : 2 557 jours

6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

7. (Facultatif) Dans Chiffrement, indiquez si vous souhaitez chiffrer l'entrepôt de données d'événement à l'aide de votre propre clé KMS. Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés à CloudTrail l'aide d'une clé KMS qui vous AWS appartient et qui la gère pour vous.

   Pour activer le chiffrement à l'aide de votre propre clé KMS, choisissez Utiliser ma propre AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez

votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

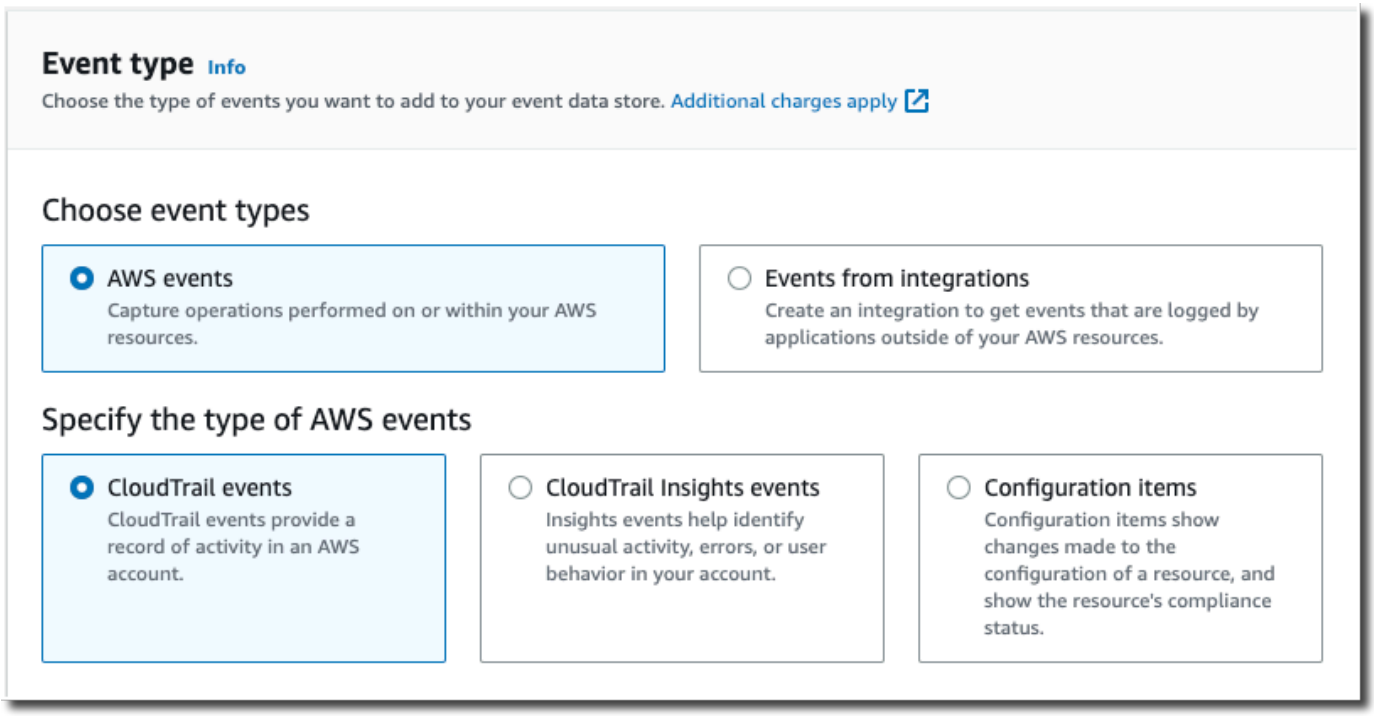
   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans Balises, ajoutez une ou plusieurs identifications personnalisées (paires valeur-clé) à votre magasin de données d'événement. Les balises peuvent vous aider à identifier les magasins de données de vos CloudTrail événements. Par exemple, il est possible d'attacher une balise portant le nom **`stage`** à la valeur **`prod`**. Vous pouvez utiliser des balises pour limiter l'accès à votre entrepôt de données d'événement. Vous pouvez également utiliser des balises pour suivre les coûts de requête et d'ingestion pour votre entrepôt de données d'événement.

   Pour plus d'informations sur l'utilisation des balises pour le suivi des coûts, veuillez consulter Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un entrepôt de données d'événement basé sur des balises, veuillez consulter Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

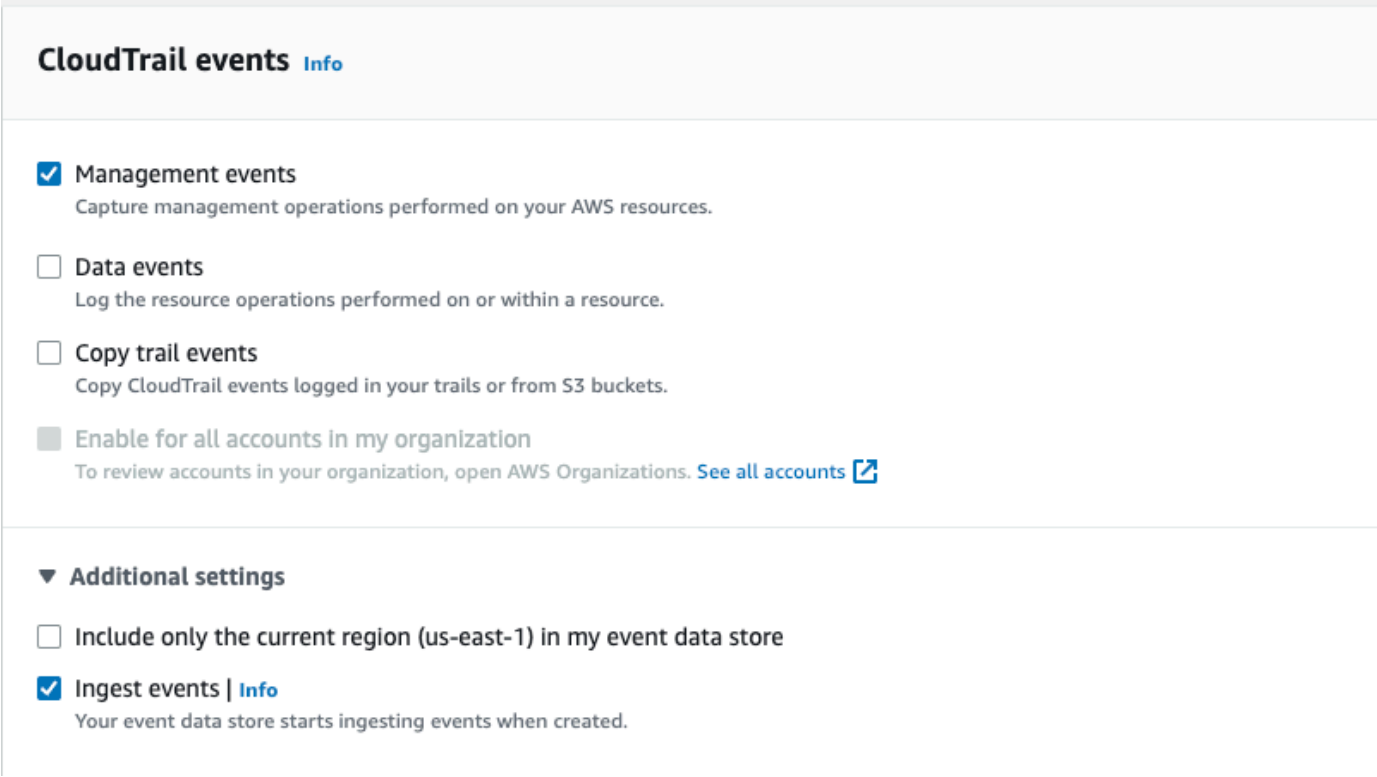
10. Choisissez Suivant pour configurer le magasin de données d'événement.

11. Sur la page Choisir des événements, conservez les sélections par défaut pour Type d'événement.

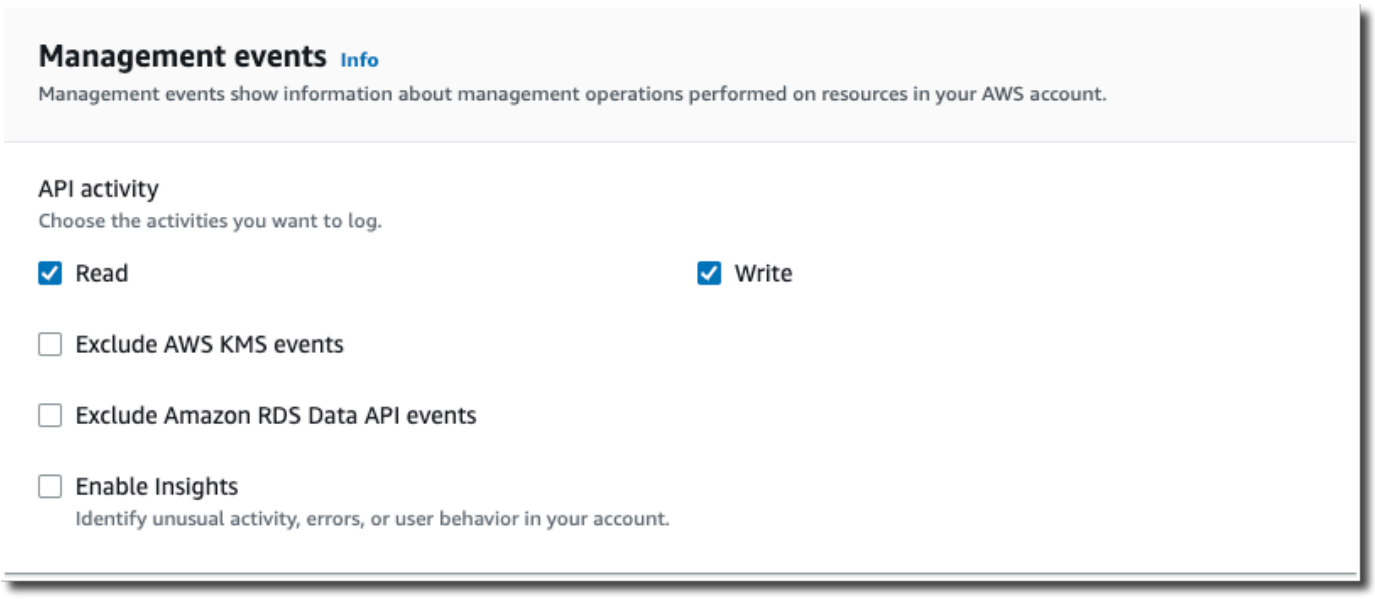


12. Pour les CloudTrail événements, conservez les sélections par défaut. Par défaut, les magasins de données d' CloudTrail événements collectent les événements de gestion et non les événements de données. Pour plus d'informations sur les événements de gestion,

veuillez consulter Journalisation des événements de gestion. Pour plus d'informations sur les événements de données, veuillez consulter Journalisation des événements de données.



13. Conservez le paramètre par défaut pour Copier les événements de suivi. Vous utiliseriez cette option pour copier des événements de journal de suivi existant dans votre entrepôt de données d'événement. Pour plus d'informations, consultez Copier des événements de journal de suivi dans un magasin de données d'événement.
14. Choisissez Activer pour tous les comptes de mon organisation s'il s'agit d'un entrepôt de données d'événement d'organisation. Cette option ne pourra pas être modifiée à moins que vous ayez des comptes configurés dans AWS Organizations.
15. Pour Paramètres supplémentaires, laissez les sélections par défaut. Par défaut, un magasin de données d'événements collecte les événements pour tous Régions AWS et commence à les ingérer dès sa création.
16. Pour Événements de gestion, choisissez de collecter à la fois les événements Lecture et Écriture. Laissez les cases à cocher Exclure les AWS KMS événements et Exclure les événements de l'API de données Amazon RDS vides pour collecter tous les événements de gestion. Ne cochez pas la case Activer les événements Insights.



17. Choisissez Suivant pour examiner vos préférences.
18. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
19. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

    À partir de ce moment, le magasin de données d'événement capture les événements qui correspondent à ses sélecteurs d'événements avancés. Les événements s'étant produits avant la création du stockage de données d'événement ne figurent pas dans celui-ci, à moins que vous ne choisissiez de copier les événements de suivi existants.

Exemple : création d'un magasin de données d'événements pour les événements de données S3

Cette procédure pas à pas explique comment créer un magasin de données d'événements pour les événements de données Amazon S3. Dans ce scénario, au lieu de consigner tous les événements liés aux données Amazon S3, nous choisirons un modèle de sélecteur de journal personnalisé pour enregistrer les événements uniquement lorsqu'un objet est supprimé d'un compartiment S3 spécifique.

Pour créer un magasin de données d'événement pour des événements S3

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.

2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configurer le magasin de données d'événements, dans Détails généraux, donnez un nom à votre magasin de données d'événements, tel que *s3- data-events-eds*. Comme bonne pratique, utilisez un nom qui identifie rapidement l'objectif de l'entrepôt de données d'événement. Pour plus d'informations sur les exigences en matière de CloudTrail dénomination, consultezExigences de dénomination.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
     - Période de conservation par défaut : 366 jours.
     - Période de conservation maximale : 3 653 jours
   - Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
     - Période de conservation par défaut : 2 557 jours.
     - Période de conservation maximale : 2 557 jours
6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez

une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

7. (Facultatif) Dans Chiffrement, indiquez si vous souhaitez chiffrer l'entrepôt de données d'événement à l'aide de votre propre clé KMS. Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés à CloudTrail l'aide d'une clé KMS qui vous AWS appartient et qui la gère pour vous.

   Pour activer le chiffrement à l'aide de votre propre clé KMS, choisissez Utiliser ma propre AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

   L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

   > **Note**
   >
   > Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.

b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.

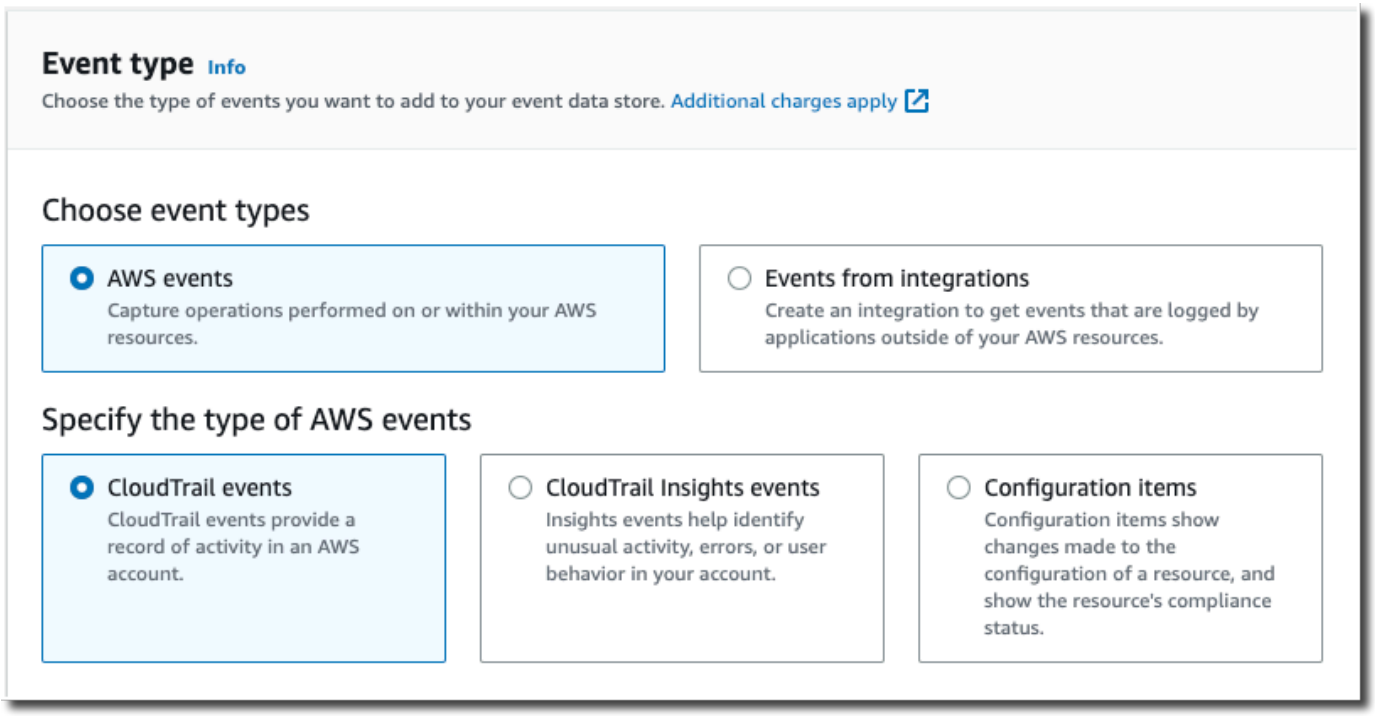
c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans Balises, ajoutez une ou plusieurs identifications personnalisées (paires valeur-clé) à votre magasin de données d'événement. Les balises peuvent vous aider à identifier les magasins de données de vos CloudTrail événements. Par exemple, il est possible d'attacher une balise portant le nom **`stage`** à la valeur **`prod`**. Vous pouvez utiliser des balises pour limiter l'accès à votre entrepôt de données d'événement. Vous pouvez également utiliser des balises pour suivre les coûts de requête et d'ingestion pour votre entrepôt de données d'événement.

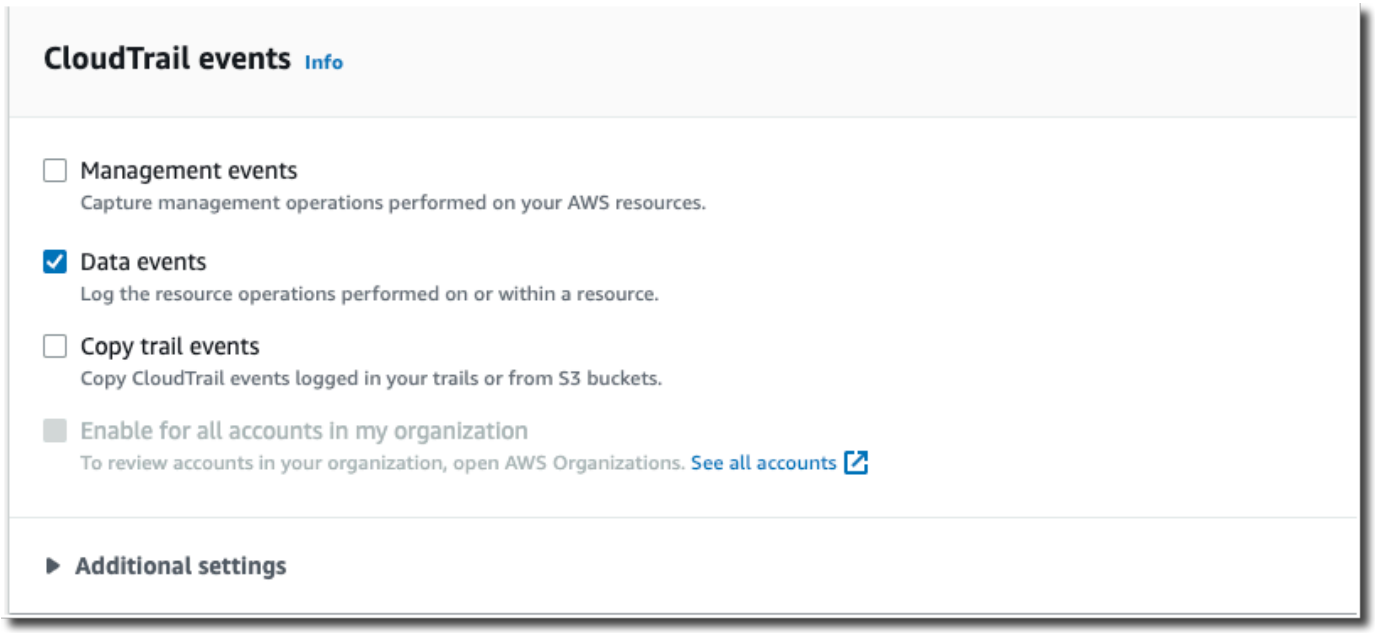
   Pour plus d'informations sur l'utilisation des balises pour le suivi des coûts, veuillez consulter Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un entrepôt de données d'événement basé sur des balises, veuillez consulter Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

10. Choisissez Suivant pour configurer le magasin de données d'événement.

11. Sur la page Choisir des événements, conservez les sélections par défaut pour Type d'événement.



12. Pour les CloudTrail événements, choisissez Data events et désélectionnez Management events. Pour plus d'informations sur les événements de données, veuillez consulter Journalisation des événements de données.



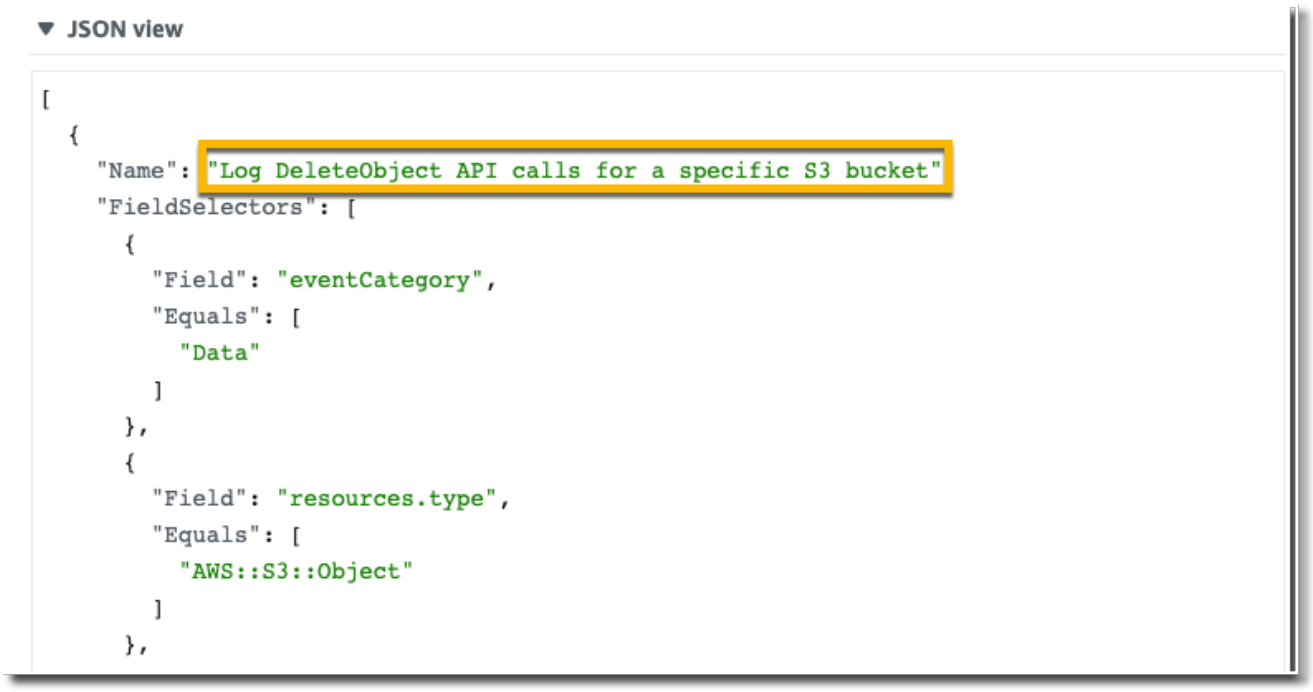
13. Conservez le paramètre par défaut pour Copier les événements de suivi. Vous utiliseriez cette option pour copier des événements de journal de suivi existant dans votre entrepôt de données d'événement. Pour plus d'informations, consultez Copier des événements de journal de suivi dans un magasin de données d'événement.

14. Choisissez Activer pour tous les comptes de mon organisation s'il s'agit d'un entrepôt de données d'événement d'organisation. Cette option ne pourra pas être modifiée à moins que vous ayez des comptes configurés dans AWS Organizations.
15. Pour Paramètres supplémentaires, laissez les sélections par défaut. Par défaut, un magasin de données d'événements collecte les événements pour tous Régions AWS et commence à les ingérer dès sa création.
16. Pour Événements de données, effectuez les sélections suivantes :

    a. Dans Type d'événement de données, choisissez S3. Le type d'événement de données identifie la ressource Service AWS et la ressource sur laquelle les événements de données sont enregistrés.

    b. Dans Modèle de sélecteur de journaux, choisissez Personnalisé. En choisissant Personnalisé, vous pouvez définir un sélecteur d'événements personnalisé pour filtrer les champs `eventName`, `resources.ARN` et `readOnly`. Pour plus d'informations sur ces champs, reportez-vous AdvancedFieldSelectorà la référence de l'AWS CloudTrail API.

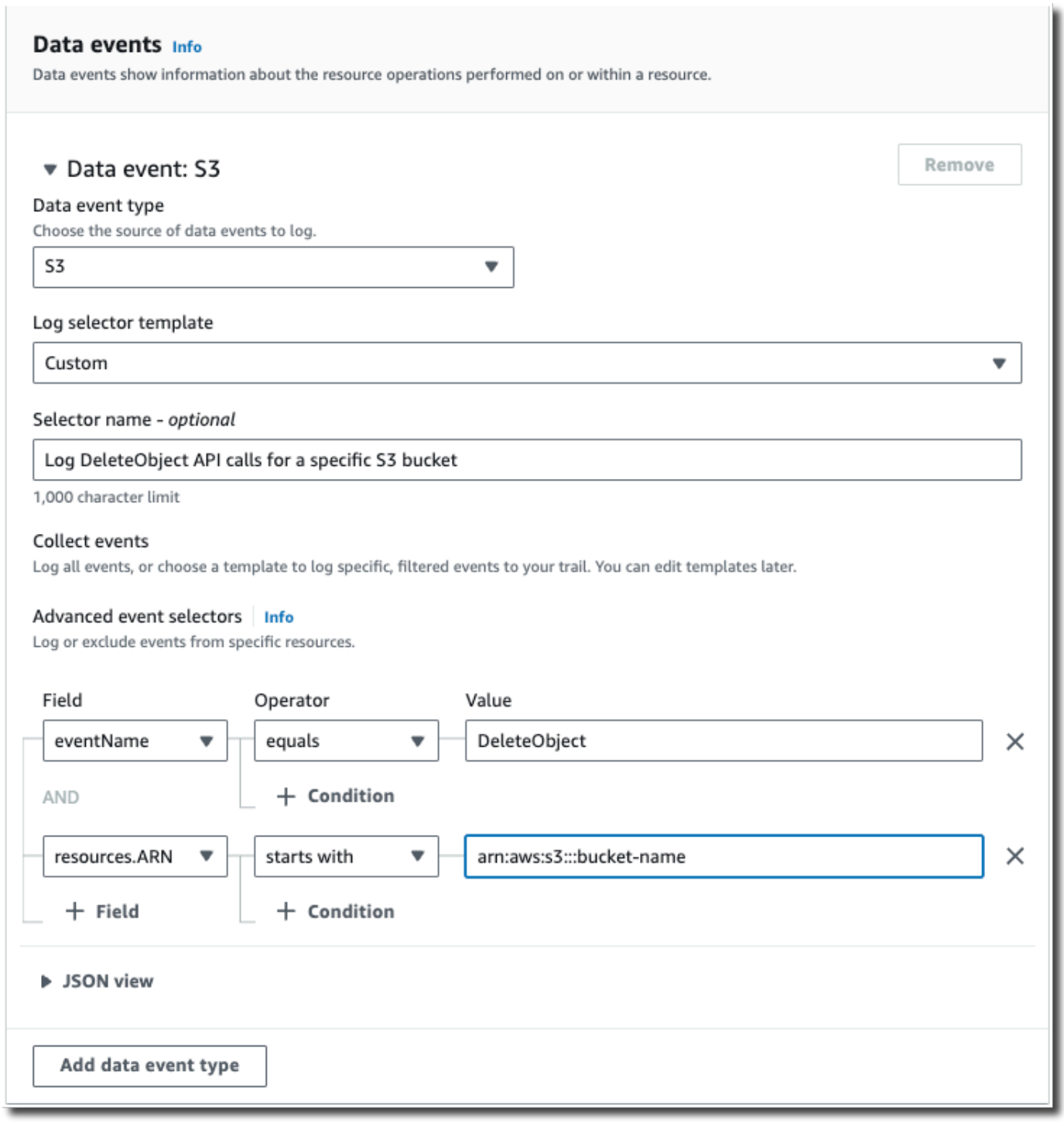
    c. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est le nom descriptif d'un sélecteur d'événements avancé, tel que « Log DeleteObject API calls for a specific S3 bucket ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.



d. Dans les sélecteurs d'événements avancés, nous allons créer le sélecteur d'événements personnalisé pour filtrer les champs `eventName` et`resources.ARN`. Les sélecteurs d'événements avancés pour un magasin de données d'événement fonctionnent de la même manière que les sélecteurs d'événements avancés que vous appliquez à un journal de suivi. Pour plus d'informations sur la création de sélecteurs d'événements avancés, consultez Journalisation des événements de données à l'aide de sélecteurs d'événement avancés.

   i. Pour Champ, choisissez eventName. Pour Opérateur, choisissez Égal à. Pour le champ Valeur, saisissez **`DeleteObject`**. Choisissez + Champ pour filtrer sur un autre champ.

   ii. Pour Champ, choisissez resources.ARN. Pour Opérateur, choisissez StartsWith. Pour Value, saisissez l'ARN de votre compartiment (par exemple, *`arn:aws:s3:::bucket-name`*). Pour plus d'informations sur la façon d'obtenir l'ARN, veuillez consulter les ressources Amazon S3 dans le Guide de l'utilisateur d'Amazon Simple Storage Service.



17. Choisissez Suivant pour examiner vos préférences.
18. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.

19. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

    À partir de ce moment, le magasin de données d'événement capture les événements qui correspondent à ses sélecteurs d'événements avancés. Les événements s'étant produits avant la création du stockage de données d'événement ne figurent pas dans celui-ci, à moins que vous ne choisissiez de copier les événements de suivi existants.

Créez un magasin de données d'événements pour les événements CloudTrail Insights à l'aide de la console

AWS CloudTrail Insights aide AWS les utilisateurs à identifier les activités inhabituelles associées aux appels d'API et aux taux d'erreur des API et à y répondre en analysant en permanence les événements CloudTrail de gestion. CloudTrail Insights analyse vos modèles habituels de volume d'appels d'API et de taux d'erreur d'API, également appelés référence, et génère des événements Insights lorsque le volume d'appels ou les taux d'erreur sont en dehors des modèles normaux. Les événements Insights sur le volume d'appels d'API sont générés pour les API de gestion `write`, et les événements Insights sur le taux d'erreur de l'API sont générés pour les API de gestion `read` et `write`.

Pour enregistrer les événements Insights dans CloudTrail Lake, vous avez besoin d'un magasin de données d'événements de destination qui enregistre les événements Insights et d'un magasin de données d'événements source qui active Insights et enregistre les événements de gestion.

> **Note**
>
> Pour enregistrer les événements Insights sur le volume d'appels d'API, l'entrepôt de données d'événement source doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, l'entrepôt de données d'événement source doit enregistrer les événements de gestion `read` ou `write`.

Si CloudTrail Insights est activé sur un magasin de données d'événements source et que vous CloudTrail détectez une activité inhabituelle, CloudTrail transmet les événements Insights à votre magasin de données d'événements de destination. Contrairement aux autres types d'événements capturés dans un magasin de données d' CloudTrail événements, les événements Insights sont enregistrés uniquement lorsque des modifications de l'utilisation de l'API de votre compte sont CloudTrail détectées, qui diffèrent considérablement des modèles d'utilisation habituels du compte.

Une fois que vous avez activé CloudTrail Insights pour la première fois dans un magasin de données d'événements, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée.

CloudTrail Insights analyse les événements de gestion qui se produisent dans une seule région, et non à l'échelle mondiale. Un événement CloudTrail Insights est généré dans la même région que les événements de gestion connexes.

Dans le cas d'un magasin de données sur les événements d'une organisation, il CloudTrail analyse les événements de gestion du compte de chaque membre au lieu d'analyser l'agrégation de tous les événements de gestion de l'organisation.

Des frais supplémentaires s'appliquent pour l'ingestion d'événements Insights à CloudTrail Lake. Vous serez facturé séparément si vous activez Insights pour les magasins de données sur les événements sur les sentiers et sur le CloudTrail lac. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Rubriques

Pour créer un entrepôt de données d'événement de destination qui journalise les événements Insights

Lorsque vous créez un entrepôt de données d'événement Insights, vous avez la possibilité de choisir un entrepôt de données d'événement source existant qui journalise les événements de gestion, puis de spécifier les types d'événements Insights que vous souhaitez recevoir. Vous pouvez également activer Insights sur un entrepôt de données d'événement nouveau ou existant après avoir créé votre entrepôt de données d'événement Insights, puis choisir cet entrepôt de données d'événement comme entrepôt de données d'événement de destination.

Cette procédure explique comment créer un entrepôt de données d'événement de destination qui journalise les événements Insights.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, ouvrez le sous-menu Lake, puis sélectionnez Entrepôts de données d'événement.

3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configure event data store (Configurer un magasin de données d'événement), dans General details (Détails généraux), saisissez un nom pour le magasin de données d'événement. Un nom est obligatoire.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
     - Période de conservation par défaut : 366 jours.
     - Période de conservation maximale : 3 653 jours
   - Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
     - Période de conservation par défaut : 2 557 jours.
     - Période de conservation maximale : 2 557 jours
6. Spécifiez une période de conservation pour le magasin de données d'événement en jours. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans. Le magasin de données d'événement conserve les données d'événement pendant le nombre de jours spécifié.
7. (Facultatif) Pour activer le chiffrement en utilisant AWS Key Management Service, choisissez Utiliser le mien AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des

CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.

   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.

   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans la zone Balises, vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre magasin de données d'événement.

Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

10. Choisissez Suivant pour configurer le magasin de données d'événement.
11. Sur la page Choisir des événements, choisissez AWS des événements, puis choisissez CloudTraildes événements Insights.
12. Dans les événements CloudTrail Insights, procédez comme suit.

    a. Choisissez Autoriser l'accès administrateur délégué si vous souhaitez accorder à l'administrateur délégué de votre organisation l'accès à cet entrepôt de données d'événement. Cette option n'est disponible que si vous êtes connecté avec le compte de gestion d'une AWS Organizations organisation.

    b. (Facultatif) Choisissez un entrepôt de données d'événement source existant qui journalise les événements de gestion et spécifiez les types Insights que vous souhaitez recevoir.

       Pour ajouter un entrepôt de données d'événement source, procédez comme suit.

       i. Choisissez Ajouter un entrepôt de données d'événement source.

       ii. Choisissez l'entrepôt de données d'événement source.

       iii. Choisissez le Type Insights que vous souhaitez recevoir.

            - `ApiCallRateInsight` : le type Insights `ApiCallRateInsight` analyse les appels à l'API de gestion en écriture seule qui sont agrégés par minute par rapport à un volume d'appels à l'API de référence. Pour recevoir des événements Insights de type `ApiCallRateInsight`, l'entrepôt de données d'événement source doit journaliser les événements de gestion Écriture.
            - `ApiErrorRateInsight` : le type Insight `ApiErrorRateInsight` analyse les appels des API de gestion qui génèrent des codes d'erreur. L'erreur s'affiche en cas d'échec de l'appel d'API. Pour recevoir des événements Insights de type `ApiErrorRateInsight`, l'entrepôt de données d'événement source doit journaliser les événements de gestion Écriture ou Lecture.

       iv. Répétez les deux étapes précédentes (ii et iii) pour ajouter les types Insights supplémentaires que vous souhaitez recevoir.

13. Choisissez Suivant pour examiner vos préférences.
14. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
15. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.
16. Si vous n'avez pas choisi d'entrepôt de données d'événement source à l'étape 10, suivez les étapes décrites dans Pour créer un entrepôt de données d'événement source qui active les événements Insights pour créer un entrepôt de données d'événement source.

Pour créer un entrepôt de données d'événement source qui active les événements Insights

Cette procédure explique comment créer un entrepôt de données d'événement source qui active les événements Insights et journalise les événements de gestion.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, ouvrez le sous-menu Lake, puis sélectionnez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configure event data store (Configurer un magasin de données d'événement), dans General details (Détails généraux), saisissez un nom pour le magasin de données d'événement. Un nom est obligatoire.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366

jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.

- Période de conservation par défaut : 366 jours.
- Période de conservation maximale : 3 653 jours

- Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
  - Période de conservation par défaut : 2 557 jours.
  - Période de conservation maximale : 2 557 jours

6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

7. (Facultatif) Pour activer le chiffrement en utilisant AWS Key Management Service, choisissez Utiliser le mien AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

   L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans la zone Balises, vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre magasin de données d'événement. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.
10. Choisissez Suivant pour configurer le magasin de données d'événement.

11. Sur la page Choisir des événements, choisissez AWS des événements, puis CloudTraildes événements.
12. Dans CloudTrail Événements, laissez la case Événements de gestion sélectionnée.
13. Pour que votre magasin de données d'événement collecte les événements de tous les comptes d'une organisation AWS Organizations , sélectionnez Activer pour tous les comptes de mon organisation. Vous devez être connecté au compte de gestion de l'organisation pour créer un entrepôt de données d'événement qui active Insights.
14. Développez les paramètres supplémentaires pour choisir si vous souhaitez que votre banque de données d'événements collecte les événements pour tous Régions AWS ou uniquement les événements actuels Région AWS, et choisissez si la banque de données d'événements ingère les événements. Par défaut, votre entrepôt de données d'événement collecte les événements de toutes les régions de votre compte et commence à ingérer les événements dès sa création.

    a. Choisissez Inclure uniquement la région actuelle dans mon entrepôt de données d'événement si vous souhaitez n'inclure que les événements journalisés dans la région actuelle. Si vous ne choisissez pas cette option, votre magasin de données d'événement inclura des événements de toutes les régions.

    b. Laissez l'option Ingérer les événements sélectionnée.
15. Choisissez le type d'événements de gestion que vous souhaitez inclure dans votre entrepôt de données d'événement. Vous pouvez choisir Lecture, Écriture ou les deux. Au moins une unité est obligatoire.

    > **Note**
    >
    > Pour enregistrer les événements Insights sur le volume d'appels d'API, l'entrepôt de données d'événement doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, l'entrepôt de données d'événement doit enregistrer les événements ou les événements de gestion `read` ou `write`.
16. Vous pouvez choisir d'exclure AWS Key Management Service ou d'exclure les événements de l'API Amazon RDS Data de votre banque de données d'événements. Pour plus d'informations sur ces options, consultez Journalisation des événements de gestion.
17. Choisissez Activer Insights.
18. Dans Activer Insights, choisissez le stockage d'événements de destination qui enregistrera les événements Insights. L'entrepôt de données d'événement de destination collectera les

événements Insights en fonction de l'activité de gestion des événements dans cet entrepôt de données d'événement. Pour plus d'informations sur la création de l'entrepôt de données événements de destination, veuillez consulter Pour créer un entrepôt de données d'événement de destination qui journalise les événements Insights.

19. Choisissez les types Insights. Vous pouvez choisir le Taux d'appels d'API, le Taux d'erreur de l'API ou les deux. Vous devez journaliser les événements de gestion Écriture pour journaliser les événements Insights afin de connaître le Taux d'appels d'API. Vous devez journaliser les événements de gestion Lecture ou Écriture pour journaliser les événements Insights afin de connaître le Taux d'erreur de l'API.
20. Choisissez Suivant pour examiner vos préférences.
21. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
22. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

    À partir de ce moment, le magasin de données d'événement capture les événements qui correspondent à ses sélecteurs d'événements avancés. Une fois que vous avez activé CloudTrail Insights pour la première fois sur votre banque de données d'événements source, la transmission du premier événement Insights CloudTrail à votre banque de données d'événements de destination peut prendre jusqu'à 7 jours, si une activité inhabituelle est détectée.

    Vous pouvez consulter le tableau de bord CloudTrail Lake pour visualiser les événements Insights dans votre banque de données d'événements de destination. Pour de plus amples informations sur le tableau de bord Lake, veuillez consulter Afficher les tableaux de bord de CloudTrail Lake.

Des frais supplémentaires s'appliquent pour l'ingestion d'événements Insights à CloudTrail Lake. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Créez un magasin de données d'événements pour les éléments AWS Config de configuration à l'aide de la console

Vous pouvez créer un entrepôt de données d'événement pour inclure des éléments de configuration AWS Config et utiliser l'entrepôt de données d'événement pour examiner les modifications non conformes apportées à vos environnements de production. Avec un magasin de données d'événement, vous pouvez associer les règles non conformes aux utilisateurs et aux ressources associés aux modifications. Un élément de configuration représente une point-in-time vue des attributs d'une AWS ressource prise en charge qui existe dans votre compte. AWS Config crée un élément de configuration chaque fois qu'il détecte une modification d'un type de ressource qu'il enregistre. AWS Config crée également des éléments de configuration lorsqu'un instantané de configuration est capturé.

Vous pouvez utiliser les deux AWS Config et CloudTrail Lake pour exécuter des requêtes sur vos éléments de configuration. Vous pouvez l'utiliser AWS Config pour interroger l'état de configuration actuel des AWS ressources en fonction des propriétés de configuration d'un seul Compte AWS ou de plusieurs comptes et régions. Région AWS En revanche, vous pouvez utiliser CloudTrail Lake pour effectuer des requêtes sur diverses sources de données telles que CloudTrail des événements, des éléments de configuration et des évaluations de règles. CloudTrail Les requêtes Lake couvrent tous les éléments AWS Config de configuration, y compris la configuration des ressources et l'historique de conformité.

La création d'un magasin de données d'événements pour les éléments de configuration n'a aucune incidence sur les requêtes AWS Config avancées existantes, ni sur AWS Config les agrégateurs configurés. Vous pouvez continuer à exécuter des requêtes avancées en utilisant AWS Config des fichiers d'historique et en AWS Config continuant de les fournir à vos compartiments S3.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Limites

Les limites suivantes s'appliquent aux magasins de données d'événement pour les éléments de configuration.

- Aucune prise en charge des éléments de configuration personnalisés
- Aucune prise en charge du filtrage d'événement à l'aide de sélecteurs d'événements avancés

Prérequis

Avant de créer votre banque de données d'événements, configurez AWS Config l'enregistrement pour tous vos comptes et régions. Vous pouvez utiliser Quick Setup, une fonctionnalité de AWS Systems Manager, pour créer rapidement un enregistreur de configuration alimenté par AWS Config.

> **Note**
>
> Des frais d'utilisation du service vous sont facturés lorsque vous AWS Config commencez à enregistrer des configurations. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Config. Pour en savoir plus sur la gestion de l'enregistreur de configuration, consultez Managing the Configuration Recorder (Gestion de l'enregistreur de configuration) dans le Guide du développeur AWS Config .

En outre, les actions suivantes sont recommandées, mais ne sont pas obligatoires pour créer un magasin de données d'événement.

- Configurez un compartiment Amazon S3 pour recevoir un instantané de configuration sur demande et un historique de configuration. Pour plus d'informations sur les instantanés, consultez Managing the Delivery Channel (Gestion du canal d'envoi) et Delivering Configuration Snapshot to an Amazon S3 Bucket (Envoi d'un instantané de configuration à un compartiment Amazon S3) dans le Guide du développeur AWS Config .
- Spécifiez les règles que vous souhaitez utiliser AWS Config pour évaluer les informations de conformité pour les types de ressources enregistrés. Plusieurs exemples de requêtes CloudTrail Lake AWS Config nécessitent d' AWS Config Rules évaluer l'état de conformité de vos AWS ressources. Pour plus d'informations AWS Config Rules, consultez la section Évaluation des ressources avec AWS Config Rules dans le Guide du AWS Config développeur.

Créer un magasin de données d'événement pour les éléments de configuration

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.

3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configure event data store (Configurer un magasin de données d'événement), dans General details (Détails généraux), saisissez un nom pour le magasin de données d'événement. Un nom est obligatoire.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
     - Période de conservation par défaut : 366 jours.
     - Période de conservation maximale : 3 653 jours
   - Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
     - Période de conservation par défaut : 2 557 jours.
     - Période de conservation maximale : 2 557 jours
6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.
7. (Facultatif) Pour activer le chiffrement en utilisant AWS Key Management Service, choisissez Utiliser le mien AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour

vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/ MyAliasName`. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans la zone Balises, vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre magasin de données d'événement. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.
10. Choisissez Suivant.
11. Sur la page Choisir les événements, sélectionnez Événements AWS , puis Éléments de configuration.
12. CloudTrail stocke la ressource du magasin de données d'événements dans la région dans laquelle vous l'avez créée, mais par défaut, les éléments de configuration collectés dans le magasin de données proviennent de toutes les régions de votre compte dont l'enregistrement est activé. En option, vous pouvez sélectionner Include only the current region in my event data store (Inclure uniquement la région actuelle dans mon magasin de données d'événement) pour inclure uniquement les éléments de configuration qui sont capturés dans la région actuelle. Si vous ne choisissez pas cette option, votre magasin de données d'événement inclut les éléments de configuration de toutes les régions dont l'enregistrement est activé.
13. Pour que votre banque de données événementielles collecte les éléments de configuration de tous les comptes d'une AWS Organizations organisation, sélectionnez Activer pour tous les comptes de mon organisation. Vous devez être connecté au compte de gestion ou au compte d'administrateur délégué de l'organisation pour créer un magasin de données d'événement qui collecte les éléments de configuration pour une organisation.
14. Choisissez Next (Suivant) pour examiner vos préférences.
15. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
16. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

    À partir de ce moment, le magasin de données d'événement capture les éléments de configuration. Les éléments de configuration qui ont eu lieu avant que vous ne créiez le magasin de données d'événement ne sont pas dans le magasin de données d'événement.

Exemples de requêtes

Vous pouvez désormais exécuter des requêtes sur votre magasin de données d'événement. L'onglet Exemples de requêtes de la CloudTrail console fournit des exemples de requêtes pour vous aider à démarrer. Vous trouverez ci-dessous quelques exemples de requêtes que vous pouvez exécuter sur le magasin de données d'événement de votre élément de configuration.

Description	Requête
Trouvez quel utilisateur a effectué une action qui a entraîné un statut de non-conformité en joignant un magasin de données d'événements d'un élément de configuration à un magasin de données d' CloudTrail événements.	`SELECT element_at(config1.eventData.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventData.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM config_event_data_store_ID as config1 JOIN config_event_data_store_ID as config2 on element_at(config1.eventData.configuration, 'targetResourceId') = config2.eventData.resourceId JOIN cloudtrail_event_data_store_ID as cloudtrail on config2.eventData.arn = element_at(cloudtrail.resources, 1).arn WHERE element_at(config1.eventData.configuration, 'configRuleList') is not null AND element_at(config1.eventData.configuration, 'complianceType') = 'NON_COMPLIANT' AND`

Description	Requête
	`cloudtrail.eventTime > '2022-11-14 00:00:00' AND config2.eventData.resourceType = 'AWS::DynamoDB::Table'`
Trouvez toutes les AWS Config règles et renvoyez l'état de conformité à partir des éléments de configuration générés le jour précédent.	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceName, eventData.resourceCreationTime, element_at(eventData.configuration,'complianceType') AS complianceType, element_at(eventData.configuration, 'configRuleList') AS configRuleList, element_at(eventData.configuration, 'resourceId') AS resourceId, element_at(eventData.configuration, 'resourceType') AS resourceType FROM config_event_data_store_ID WHERE eventData.resourceType = 'AWS::Config::ResourceCompliance' AND eventTime > '2022-11-22 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10`

Description	Requête
Trouvez le nombre total de AWS Config ressources regroupées par type de ressource, ID de compte et région.	`SELECT eventData.resourceType, eventData.awsRegion, eventData.accountId, COUNT (*) AS resourceCount FROM config_event_data_store_ID WHERE eventTime > '2022-11-22 00:00:00' GROUP BY eventData.resourceType, eventData.awsRegion, eventData.accountId`
Trouvez l'heure de création des ressource s pour tous les éléments de AWS Config configuration générés à une date précise.	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceId, eventData.resourceName, eventData.resourceType, eventData.availabilityZone, eventData.resourceCreationTime FROM config_event_data_store_ID WHERE eventTime > '2022-11-16 00:00:00' AND eventTime < '2022-11-17 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10;`

Pour plus d'informations sur la création et la modification des requêtes, consultez Créer ou modifier une requête.

Schéma des éléments de configuration

Le tableau suivant décrit les éléments de schéma obligatoires et facultatifs qui correspondent à ceux des enregistrements d'éléments de configuration. Le contenu de `eventData` est fourni par vos éléments de configuration ; les autres champs sont fournis par CloudTrail après ingestion.

CloudTrail le contenu des enregistrements d'événements est décrit plus en détail dansCloudTrail enregistrer le contenu.

- Champs fournis par CloudTrail After ingestion
- Champs fournis par vos événements

Champs fournis par CloudTrail After ingestion

Nom de champ	Type d'entrée	Exigence	Description
eventVersion	chaîne	Obligatoire	Version du format de l' AWS événement.
eventCategory	chaîne	Obligatoire	Catégorie de l'événement. Pour les éléments de configuration, la valeur valide est `ConfigurationItem` .
eventType	chaîne	Obligatoire	Type d'événement. Pour les éléments de configuration, la valeur valide est `AwsConfigurationItem` .
eventID	chaîne	Obligatoire	ID unique pour un événement.
eventTime	chaîne	Obligatoire	L'horodatage de l'événement, au format `yyyy-MM-`

Nom de champ	Type d'entrée	Exigence	Description
			DDTHH:mm:ss , en temps universel coordonné (UTC).
awsRegion	chaîne	Obligatoire	Région AWS À laquelle attribuer un événement.
recipientAccountId	chaîne	Obligatoire	Représente l' Compte AWS ID qui a reçu cet événement.
addendum	addendum	Facultatif	Affiche des informations sur la raison pour laquelle un événement a été retardé. Si des informations manquaient dans un événement existant, le bloc d'addendum inclut les informations manquantes et la raison de leur absence.

Les champs dans **`eventData`** sont fournis par vos éléments de configuration

Nom de champ	Type d'entrée	Exigence	Description
eventData	-	Obligatoire	Les champs de eventData sont fournis par vos éléments de configuration.

Nom de champ	Type d'entrée	Exigence	Description
• configurationItemVersion	chaîne	Facultatif	Version de l'élément de configuration provenant de sa source.
• configurationItemCaptureHeure	chaîne	Facultatif	Heure à laquelle l'enregistrement de configuration a été lancé.
• configurationItemStatus	chaîne	Facultatif	Statut de l'élément de configuration. Les valeurs valides sont OK, `ResourceDiscovered` , `ResourceNotRecorded` , `ResourceDeleted` et `ResourceDeletedNotRecorded` .
• accountId	chaîne	Facultatif	L' Compte AWS identifiant à 12 chiffres associé à la ressource.
• resourceType	chaîne	Facultatif	Type de AWS ressource. Pour plus d'informations sur les types de ressources valides, consultez ConfigurationItemla référence de l'AWS Config API.

Nom de champ	Type d'entrée	Exigence	Description
• resourceId	chaîne	Facultatif	ID de la ressource (par exemple, sg-*xxxxxx*).
• resourceName	chaîne	Facultatif	Nom personnalisé de la ressource, si disponible.
• arn	chaîne	Facultatif	Amazon Resource Name (ARN) associé à la ressource.
• awsRegion	chaîne	Facultatif	L' Région AWS endroit où se trouve la ressource.
• availabilityZone	chaîne	Facultatif	Zone de disponibilité associée à la ressource.
• resourceCreationTime	chaîne	Facultatif	Horodatage de la création de la ressource.
• configuration	JSON	Facultatif	Description de la configuration de la ressource.

Nom de champ	Type d'entrée	Exigence	Description
• supplementaryConfiguration	JSON	Facultatif	Attributs de configuration AWS Config renvoyés pour certains types de ressources afin de compléter les informations renvoyées pour le paramètre de configuration.
• relatedEvents	chaîne	Facultatif	Liste des identifiants d' CloudTrail événements.
• relationships	-	Facultatif	Une liste de AWS ressources connexes.
• • name	chaîne	Facultatif	Type de relation avec la ressource associée.
• • resourceType	chaîne	Facultatif	Type de ressource de la ressource associée.
• • resourceId	chaîne	Facultatif	ID de la ressource associée (par exemple, sg-*xxxxxx*).
• • resourceName	chaîne	Facultatif	Nom personnalisé de la ressource associée, si disponible.
• tags	JSON	Facultatif	Mappage des balises clé-valeur associées à la ressource.

L'exemple suivant montre la hiérarchie des éléments du schéma qui correspondent à ceux des enregistrements d'éléments de configuration.

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
```

```
        JSON
      }
     }
   }
}
```

Création d'un magasin de données d'événements pour les événements extérieurs AWS à la console

Vous pouvez créer un magasin de données d'événements pour inclure des événements extérieurs à AWS, puis utiliser CloudTrail Lake pour rechercher, interroger et analyser les données enregistrées par vos applications.

Vous pouvez utiliser les intégrations CloudTrail Lake pour enregistrer et stocker les données d'activité des utilisateurs provenant de l'extérieur AWS, de n'importe quelle source dans vos environnements hybrides, telles que des applications internes ou SaaS hébergées sur site ou dans le cloud, des machines virtuelles ou des conteneurs.

Lorsque vous créez un magasin de données d'événement pour une intégration, vous créez également un canal associé à une politique de ressources.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Pour créer un magasin de données d'événements pour des événements en dehors de AWS

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configure event data store (Configurer un magasin de données d'événement), dans General details (Détails généraux), saisissez un nom pour le magasin de données d'événement. Un nom est obligatoire.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des

événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

Les options suivantes sont disponibles :

- Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
  - Période de conservation par défaut : 366 jours.
  - Période de conservation maximale : 3 653 jours
- Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
  - Période de conservation par défaut : 2 557 jours.
  - Période de conservation maximale : 2 557 jours

6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

7. (Facultatif) Pour activer le chiffrement en utilisant AWS Key Management Service, choisissez Utiliser le mien AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales.

Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.

8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans la zone Balises, vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre magasin de données d'événement. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès

à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

10. Choisissez Suivant pour configurer le magasin de données d'événement.
11. Sur la page Choose events (Choisir les événements), sélectionnez Events from integrations (Événements issus des intégrations).
12. Dans Events from integration (Événements issus des intégrations), sélectionnez la source pour transmettre les événements au stockage de données d'événement.
13. Fournissez un nom afin d'identifier le canal de l'intégration. Le nom doit comporter entre 3 et 128 caractères. Les noms peuvent contenir uniquement des lettres, des chiffres, des points, des tirets et des traits de soulignement.
14. Dans Resource policy (Politique de ressources), configurez la politique de ressources pour le canal de l'intégration. Les politiques de ressources sont des documents de politique JSON précisant les actions qu'un principal spécifié peut effectuer sur la ressource ainsi que les conditions dans lesquelles ces actions peuvent être effectuées. Les comptes définis comme principaux dans la politique de ressources peuvent appeler l'API `PutAuditEvents` pour transmettre des événements à votre canal. Le propriétaire de la ressource dispose d'un accès implicite à la ressource si sa politique IAM autorise l'action `cloudtrail-data:PutAuditEvents`.

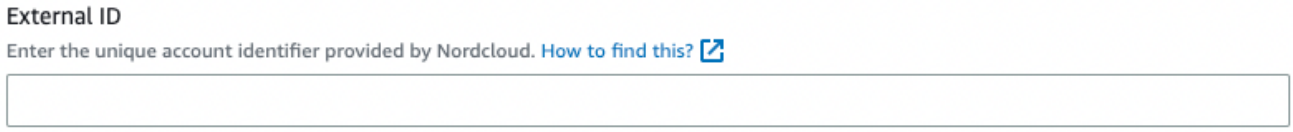
    Les informations requises pour la politique sont déterminées par le type d'intégration. Pour une intégration des directions, ajoute CloudTrail automatiquement les identifiants de AWS compte du partenaire et vous demande de saisir l'identifiant externe unique fourni par le partenaire. Pour une intégration de solution, vous devez spécifier au moins un identifiant de AWS compte comme identifiant principal, et vous pouvez éventuellement saisir un identifiant externe pour éviter toute confusion entre les adjoints.

    > **Note**
    >
    > Si vous ne créez pas de politique de ressources pour le canal, seul son propriétaire peut appeler l'API `PutAuditEvents` sur celui-ci.

    a. Pour une intégration directe, saisissez l'ID externe fourni par votre partenaire. Le partenaire d'intégration fournit un ID externe unique, tel qu'un ID de compte ou une chaîne générée

aléatoirement, à utiliser pour l'intégration afin d'éviter tout problème d'adjoint confus. Le partenaire est responsable de la création et de la transmission d'un ID externe unique.

Vous pouvez sélectionner How to find this? (Comment trouver cela ?) pour consulter la documentation du partenaire expliquant comment trouver l'ID externe.



> **Note**
>
> Si la politique de ressources inclut un ID externe, tous les appels à l'API `PutAuditEvents` doivent l'inclure. Cependant, si la politique ne définit pas d'ID externe, le partenaire peut appeler l'API `PutAuditEvents` et spécifier un paramètre `externalId`.

b. Pour une intégration de solution, choisissez Ajouter un AWS compte pour spécifier chaque ID de AWS compte à ajouter en tant que principal dans la politique.

15. Choisissez Suivant pour examiner vos préférences.
16. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
17. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.
18. Fournissez l'Amazon Resource Name (ARN) du canal à l'application partenaire. Les instructions pour fournir l'ARN du canal à l'application partenaire se trouvent sur le site Web de documentation du partenaire. Afin d'obtenir davantage d'informations et ouvrir la page du partenaire dans AWS Marketplace, cliquez sur le lien Learn more (En savoir plus) pour le partenaire dans l'onglet Available sources (Sources disponibles) de la page Integrations (Intégrations).

Le magasin de données d'événements commence à intégrer les événements des partenaires CloudTrail via le canal de l'intégration lorsque vous, le partenaire ou les applications partenaires appelez l'`PutAuditEvents`API sur le canal.

Mettre à jour un magasin de données d'événements avec la console

Cette section décrit comment mettre à jour les paramètres d'un magasin de données d'événement à l'aide de l' AWS Management Console. Pour plus d'informations sur la mise à jour d'une banque de données d'événements à l'aide du AWS CLI, voirMettez à jour un magasin de données d'événements avec AWS CLI.

Pour mettre à jour un magasin de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Magasins de données d'événement.
3. Choisissez le magasin de données d'événement que vous voulez mettre à jour. Cette action ouvre la page contenant les détails du magasin de données d'événement.
4. Dans Renseignements généraux, choisissez Modifier pour modifier les paramètres suivants :

   - Nom du magasin de données d'événement : modifiez le nom qui identifie votre magasin de données d'événement.
   - Option de tarification : pour les magasins de données d'événement utilisant l'option de tarification de rétention sur sept ans, vous pouvez choisir d'utiliser plutôt une tarification de rétention extensible d'un an. Nous recommandons une tarification de rétention extensible d'un an pour les magasins de données d'événement qui ingèrent moins de 25 To de données d'événements par mois. Nous recommandons également une tarification de rétention extensible d'un an si vous recherchez une période de rétention flexible allant jusqu'à 10 ans. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

     > **Note**
     >
     > Vous ne pouvez pas modifier l'option de tarification pour les magasins de données d'événement qui utilisent une tarification de rétention extensible d'un an. Si vous souhaitez utiliser la tarification de rétention sur sept ans, arrêtez l'ingestion dans votre magasin de données d'événement actuel. Créez ensuite un nouveau magasin de données d'événement avec l'option de tarification de rétention sur sept ans.

   - Période de conservation : modifiez la période de conservation du magasin de données d'événement. La période de conservation détermine la durée pendant laquelle les données

d'événement sont conservées dans le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

> **Note**
>
> Si vous réduisez la période de conservation d'une banque de données d'événements, vous CloudTrail supprimerez tous les événements dont la période de conservation est `eventTime` antérieure à la nouvelle. Par exemple, si la période de conservation précédente était de 365 jours et que vous la réduisez à 100 jours, les événements datant de `eventTime` plus de 100 jours CloudTrail seront supprimés.

- Chiffrement : pour chiffrer votre magasin de données d'événement à l'aide de votre propre clé KMS, choisissez Utiliser ma propre AWS KMS key. Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés par CloudTrail. L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement.

> **Note**
>
> Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

- Pour n'inclure que les événements journalisés dans l' Région AWS actuelle, sélectionnez Inclure uniquement la région actuelle dans mon magasin de données d'événement. Si vous ne choisissez pas cette option, votre magasin de données d'événement inclura des événements de toutes les régions.
- Pour que votre banque de données d'événements collecte les événements de tous les comptes d'une AWS Organizations organisation, choisissez Activer pour tous les comptes de mon organisation. Cette option n'est disponible que si vous êtes connecté avec le compte de gestion de votre organisation et que le type d'événement pour le magasin de données d'CloudTrailévénements est événements ou éléments de configuration.

Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

5. Dans Fédération de requêtes Lake, choisissez Modifier pour activer ou désactiver la fédération de requêtes Lake. L'activation de la fédération de requêtes Lake vous permet de consulter les métadonnées de votre banque de données d'événements dans le catalogue de AWS Glue

données et d'exécuter des requêtes SQL sur les données d'événements à l'aide d'Amazon Athena. La désactivation de la fédération de requêtes Lake désactive l'intégration avec AWS Glue AWS Lake Formation, et Amazon Athena. Après avoir désactivé la fédération de requêtes Lake, vous ne pouvez plus interroger vos données dans Athena. Aucune donnée de CloudTrail Lake n'est supprimée lorsque vous désactivez la fédération et vous pouvez continuer à exécuter des requêtes dans CloudTrail Lake.

Pour activer la fédération, procédez comme suit :

a. Sélectionnez Activer.

b. Choisissez de créer un nouveau rôle IAM ou d'utiliser un rôle IAM existant. Lorsque vous créez un nouveau rôle, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous utilisez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.

c. Si vous créez un nouveau rôle IAM, saisissez un nom pour identifier le rôle.

d. Si vous choisissez un rôle IAM existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

Lorsque vous avez terminé, choisissez Enregistrer les modifications.

6. Modifiez tous les paramètres supplémentaires pour votre type d'événement.

Type d'événement	Paramètres modifiables
CloudTrail événements	Vous pouvez modifier les paramètres suivants pour les CloudTrail événements : • Pour modifier les événements que vos données d'événements enregistrent, choisissez Modifier dans les CloudTrail événements. • Dans Événements de gestion, choisisse z Modifier pour modifier les paramètres des événements de gestion. Pour de plus amples informations, veuillez consulter Enregistrement des événements de

Type d'événement	Paramètres modifiables
	gestion à l'aide du AWS Management Console (étape 3). • Dans Événements de données, choisissez Modifier pour modifier les paramètres des événements de données. Vous pouvez choisir les types d'événements de données que vous souhaitez enregistrer et le modèle de sélecteur de journal que vous souhaitez utiliser. Pour plus d'informations, consultez Mettre à jour un magasin de données d'événements existant pour consigner les événements de données dans AWS Management Console. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Type d'événement	Paramètres modifiables
Événements issus de l'intégration	Dans Intégrations, choisissez votre intégrati on. Puis choisissez Modifier pour modifier les paramètres suivants : • Dans Détails de l'intégration, modifiez le nom qui identifie le canal de votre intégrati on. • Dans Emplacement de réception des événements, choisissez la destination de vos événements. • Dans Politique de ressources, configurez la politique de ressources pour le canal de l'intégration. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications. Pour plus d'informations sur ces paramètre s, consultez la page Créez une intégration avec une source d'événements en dehors de AWS.

7. Pour ajouter, modifier ou supprimer des balises, choisissez Modifier dans Balises. Vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre magasin de données d'événement. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Arrêter et démarrer l'ingestion d'événements avec la console

Par défaut, les magasins de données d'événement sont configurés pour ingérer des événements. Vous pouvez empêcher un magasin de données d'événements d'ingérer des événements à l'aide de la console ou AWS CLI des API.

Les options permettant de démarrer l'ingestion et d'arrêter l'ingestion ne sont disponibles que sur les magasins de données d'événements contenant soit des CloudTrail événements (événements de gestion et de données), soit des éléments AWS Config de configuration.

Lorsque vous arrêtez l'ingestion sur un entrepôt de données d'événement, l'état de l'entrepôt de données d'événement passe à `STOPPED_INGESTION`. Vous pouvez toujours exécuter des requêtes sur des événements déjà présents dans l'entrepôt de données d'événement. Vous pouvez également copier les événements de suivi dans le magasin de données d'événements (s'il ne contient que CloudTrail des événements de gestion ou de données).

Pour arrêter l'ingestion d'événements par un entrepôt de données d'événements

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.
4. Dans Actions, choisissez Arrêter l'ingestion.
5. Lorsque vous êtes invité à confirmer, choisissez Oui. L'entrepôt de données d'événement cessera d'ingérer les événements en direct.
6. Pour reprendre l'ingestion, sélectionnez Démarrer l'ingestion.

Pour redémarrer l'ingestion d'événements

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.
4. Dans Actions, choisissez Arrêter l'ingestion.

Modifier la protection contre le licenciement à l'aide de la console

Par défaut, les magasins de données d'événements de AWS CloudTrail Lake sont configurés avec la protection de terminaison activée. La protection contre la résiliation empêche la suppression accidentelle d'un magasin de données d'événement. Si vous souhaitez supprimer le magasin de données d'événement, vous devez désactiver la protection contre la résiliation. Vous pouvez

désactiver la protection contre les résiliations à l'aide des opérations AWS Management Console AWS CLI, ou de l'API.

Pour désactiver la protection contre la résiliation

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.
4. Choisissez Actions, puis Changer la protection contre la résiliation.
5. Choisissez Désactiver.
6. Choisissez Enregistrer. Vous pouvez désormais supprimer le magasin de données d'événement.

Pour activer la protection contre la résiliation

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.
4. Choisissez Actions, puis Changer la protection contre la résiliation.
5. Pour activer la protection contre la résiliation, choisissez Activé.
6. Choisissez Enregistrer.

Supprimer un magasin de données d'événements à l'aide de la console

Cette section décrit comment supprimer un magasin de données d'événement à l'aide de la console AWS CloudTrail . Pour plus d'informations sur la suppression d'une banque de données d'événements à l'aide du AWS CLI, voirSupprimer un magasin de données d'événements à l'aide du AWS CLI.

> **Note**
>
> Vous ne pouvez pas supprimer un magasin de données d'événement si la protection contre la résiliation ou la fédération de requêtes Lake sont activées. CloudTrail Active par défaut la protection contre les interruptions pour empêcher la suppression accidentelle d'un magasin de données d'événements.

Pour supprimer un magasin de données d'événement dont le type d'événement est Événements issus de l'intégration vous devez d'abord supprimer le canal de l'intégration. Vous pouvez supprimer le canal depuis la page de détails de l'intégration ou à l'aide de la commande aws cloudtrail delete-channel. Pour de plus amples informations, veuillez consulter la page Supprimer une chaîne pour supprimer une intégration avec AWS CLI.

Supprimer un magasin de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.
4. Dans Actions, choisissez Supprimer.
5. Entrez le nom du magasin de données d'événement pour confirmer que vous souhaitez le supprimer.
6. Sélectionnez Delete (Supprimer).

Une fois que vous avez supprimé un magasin de données d'événement, l'état du magasin de données d'événement passe à `PENDING_DELETION` et reste dans cet état pendant 7 jours. Vous pouvez restaurer un magasin de données d'événement au cours de la période d'attente de sept jours. Lorsqu'il a l'état `PENDING_DELETION`, un magasin de données d'événement n'est pas disponible pour les requêtes et aucune autre opération ne peut être effectuée sur le magasin de données d'événement, sauf les opérations de restauration. Un magasin de données d'événement en attente de suppression n'ingère pas d'événement et n'entraîne pas de coûts. Les magasins de données d'événements en attente de suppression sont pris en compte dans le quota de magasins de données d'événements qui peuvent exister dans un seul Région AWS.

Restaurer un magasin de données d'événements à l'aide de la console

Une fois que vous avez supprimé un magasin de données d'événements dans AWS CloudTrail Lake, son statut change `PENDING_DELETION` et reste dans cet état pendant 7 jours. Pendant ce temps, vous pouvez restaurer le magasin de données d'événements à l'aide de l'opération AWS Management Console AWS CLI, ou de l'RestoreEventDataStoreAPI.

Cette section décrit comment restaurer un magasin de données d'événement à l'aide de la console. Pour plus d'informations sur la restauration d'une banque de données d'événements à l'aide du AWS CLI, voirRestaurez une banque de données d'événements à l'aide du AWS CLI.

Pour restaurer un magasin de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.
4. Depuis Actions, choisissez Restaurer.

Créez, mettez à jour et gérez des banques de données d'événements à l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour créer, mettre à jour et gérer vos magasins de données d'événements. Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la Région AWS configuration adaptée à votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

Commandes disponibles pour les magasins de données d'événements

Les commandes permettant de créer et de mettre à jour des banques de données d'événements dans CloudTrail Lake incluent :

- `create-event-data-store`pour créer un magasin de données d'événements.
- `get-event-data-store`pour renvoyer des informations sur le magasin de données d'événements, y compris les sélecteurs d'événements avancés configurés pour le magasin de données d'événements.
- `update-event-data-store`pour modifier la configuration d'un magasin de données d'événements existant.
- `list-event-data-stores`pour répertorier les magasins de données d'événements.
- `delete-event-data-store`pour supprimer un magasin de données d'événements.
- `restore-event-data-store`pour restaurer une banque de données d'événements en attente de suppression.

- `start-import`pour démarrer une importation d'événements de suivi vers une banque de données d'événements ou pour réessayer une importation qui a échoué.
- `get-import`pour renvoyer des informations relatives à une importation spécifique.
- `stop-import`pour arrêter l'importation d'événements de randonnée dans un magasin de données d'événements.
- `list-imports`pour renvoyer des informations sur toutes les importations, ou sur un ensemble sélectionné d'importations effectuées par `ImportStatus` ou`Destination`.
- `list-import-failures`pour répertorier les échecs d'importation pour l'importation spécifiée.
- `stop-event-data-store-ingestion`pour arrêter l'ingestion d'événements dans un magasin de données d'événements.
- `start-event-data-store-ingestion`pour relancer l'ingestion d'événements dans un magasin de données d'événements.
- `enable-federation`pour activer la fédération sur un magasin de données d'événements afin d'interroger le magasin de données d'événements dans Amazon Athena.
- `disable-federation`pour désactiver la fédération sur un magasin de données d'événements. Une fois la fédération désactivée, vous ne pouvez plus interroger les données du magasin de données d'événements dans Amazon Athena. Vous pouvez continuer à interroger dans CloudTrail Lake.
- `put-insight-selectors`pour ajouter ou modifier des sélecteurs d'événements Insights pour un magasin de données d'événements existant, et pour activer ou désactiver les événements Insights.
- `get-insight-selectors`pour renvoyer des informations sur les sélecteurs d'événements Insights configurés pour un magasin de données d'événements.
- `add-tags`pour ajouter une ou plusieurs balises (paires clé-valeur) à un magasin de données d'événements existant.
- `remove-tags`pour supprimer une ou plusieurs balises d'une banque de données d'événements.
- `list-tags`pour renvoyer une liste de balises associées à un magasin de données d'événements.

Pour obtenir la liste des commandes disponibles pour les requêtes CloudTrail Lake, consultezCommandes disponibles pour les requêtes CloudTrail Lake.

Pour obtenir la liste des commandes disponibles pour les intégrations de CloudTrail Lake, consultezCommandes disponibles pour les intégrations de CloudTrail Lake.

Créez un magasin de données d'événements à l'aide du AWS CLI

Utilisez la commande `create-event-data-store` pour créer un magasin de données d'événement.

Lorsque vous créez un magasin de données d'événement, le seul paramètre requis est `--name`, qui est utilisé pour identifier le magasin de données d'événement. Vous pouvez configurer des paramètres facultatifs supplémentaires, notamment :

- `--advanced-event-selectors` : Spécifie le type d'événements à inclure dans le magasin de données d'événement. Par défaut, les magasins de données d'événement journalisent tous les événements de gestion. Pour plus d'informations sur les sélecteurs d'événements avancés, consultez AdvancedEventSelectorla référence de l' CloudTrail API.
- `--kms-key-id`- Spécifie l'ID de clé AWS KMS à utiliser pour chiffrer les événements transmis par CloudTrail. La valeur peut être un nom d'alias avec le préfixe `alias/`, un ARN complet d'un alias, un ARN complet d'une clé ou un identifiant unique à l'échelle mondiale.
- `--multi-region-enabled`- Crée un magasin de données d'événements multirégional qui enregistre les événements pour tous les utilisateurs Régions AWS de votre compte. Par défaut, `--multi-region-enabled` est défini, même si le paramètre n'est pas ajouté.
- `--organization-enabled` : Permet à un magasin de données d'événement de collecter des événements pour tous les comptes d'une organisation. Le magasin de données d'événement n'est pas activé par défaut pour tous les comptes d'une organisation .
- `--billing-mode` : Détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour le magasin de données d'événement.

  Les valeurs possibles sont les suivantes :

  - `EXTENDABLE_RETENTION_PRICING` : Ce mode de facturation est généralement recommandé si vous ingérez moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 3 653 jours (environ 10 ans). La période de conservation par défaut pour ce mode de facturation est de 366 jours.
  - `FIXED_RETENTION_PRICING` : Ce mode de facturation est recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 2 557 jours (environ 7 ans). La période de conservation par défaut pour ce mode de facturation est de 2 557 jours.

  La valeur par défaut est `EXTENDABLE_RETENTION_PRICING`.

- `--retention-period` : Le nombre de jours pendant lesquels les événements doivent être conservés dans le magasin de données d'événement. Les valeurs valides sont des entiers compris entre 7 et 3 653 si le paramètre `--billing-mode` est défini sur `EXTENDABLE_RETENTION_PRICING`, ou entre 7 et 2 557 si le paramètre `--billing-mode` est défini sur `FIXED_RETENTION_PRICING`. Si vous ne le spécifiez pas`--retention-period`, CloudTrail utilise la période de conservation par défaut pour le`--billing-mode`.
- `--start-ingestion` : Le paramètre `--start-ingestion` démarre l'ingestion d'événement sur le magasin de données d'événement lors de sa création. Ce paramètre est défini même s'il n'est pas ajouté.

  Spécifiez le paramètre `--no-start-ingestion` si vous ne souhaitez pas que le magasin de données d'événement ingère des événements en direct. Par exemple, vous souhaiterez peut-être définir ce paramètre si vous copiez des événements dans le magasin de données d'événement et que vous prévoyez de n'utiliser les données d'événement que pour analyser des événements passés. Le paramètre `--no-start-ingestion` n'est valide que lorsque le paramètre `eventCategory` est défini sur `Management`, `Data` ou `ConfigurationItem`.

Les exemples suivants montrent comment créer différents types de magasins de données d'événement.

Rubriques

- Créez un magasin de données d'événements pour les événements de données S3 à l'aide du AWS CLI
- Créez un magasin de données d'événements pour les éléments AWS Config de configuration à l'aide du AWS CLI
- Créez un magasin de données sur les événements d'organisation pour la gestion des événements à l'aide du AWS CLI
- Créez des banques de données d'événements pour les événements Insights à l'aide du AWS CLI

Créez un magasin de données d'événements pour les événements de données S3 à l'aide du AWS CLI

La create-event-data-store commande example AWS Command Line Interface (AWS CLI) suivante crée un magasin de données d'événements nommé `my-event-data-store` qui sélectionne tous les événements de données Amazon S3 et est chiffré à l'aide d'une clé KMS.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
    ]'
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
```

```
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

Créez un magasin de données d'événements pour les éléments AWS Config de configuration à l'aide du AWS CLI

L'exemple de AWS CLI create-event-data-store commande suivant crée un magasin de données d'événements nommé `config-items-eds` qui sélectionne des éléments AWS Config de configuration. Pour collecter des éléments de configuration, spécifiez que le champ `eventCategory` est égal à `ConfigurationItem` dans les sélecteurs d'événements avancés.

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
```

```
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

Créez un magasin de données sur les événements d'organisation pour la gestion des événements à l'aide du AWS CLI

L'exemple de AWS CLI create-event-data-store commande suivant crée un magasin de données d'événements d'organisation qui collecte tous les événements de gestion et définit le `--billing-mode` paramètre sur`FIXED_RETENTION_PRICING`.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
```

```
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

Créez des banques de données d'événements pour les événements Insights à l'aide du AWS CLI

Pour enregistrer les événements Insights dans CloudTrail Lake, vous avez besoin d'un magasin de données d'événements de destination qui collecte les événements Insights et d'un magasin de données d'événements source qui active Insights et enregistre les événements de gestion.

Cette procédure explique comment créer les entrepôts de données d'événement de destination et d'origine, puis activer les événements Insights.

1. Exécutez la commande aws cloudtrail create-event-data-store pour créer un entrepôt de données d'événement de destination qui collecte les événements Insights. La valeur pour `eventCategory` doit être `Insight`. Remplacez *`retention-period-days`*par le nombre de jours pendant lesquels vous souhaitez conserver les événements dans votre banque de données d'événements. Les valeurs valides sont des entiers compris entre 7 et 3 653 si le paramètre `--billing-mode` est défini sur `EXTENDABLE_RETENTION_PRICING`, ou entre 7 et 2 557 si le paramètre `--billing-mode` est défini sur `FIXED_RETENTION_PRICING`. Si vous ne le spécifiez pas`--retention-period`, CloudTrail utilise la période de conservation par défaut pour le`--billing-mode`.

   Si vous êtes connecté avec le compte de gestion d'une AWS Organizations organisation, incluez le `--organization-enabled` paramètre si vous souhaitez donner à votre administrateur délégué l'accès au magasin de données d'événements.

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   ```

```
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

Voici un exemple de réponse.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

Vous utiliserez l'ARN (ou le suffixe d'ID de l'ARN) de la réponse comme valeur du paramètre `--insights-destination` à l'étape 3.

2. Exécutez la commande aws cloudtrail create-event-data-store pour créer un entrepôt de données d'événement source qui journalise les événements de gestion. Par défaut, les entrepôts de données d'événement journalisent les événements de gestion et aucun événement de données. Il n'est pas nécessaire de spécifier les sélecteurs d'événements avancés si vous souhaitez journaliser tous les événements de gestion. Remplacez *retention-period-days* par le nombre de jours pendant lesquels vous souhaitez conserver les événements dans votre banque de données d'événements. Les valeurs valides sont des entiers compris entre 7 et 3 653 si le paramètre `--billing-mode` est défini sur `EXTENDABLE_RETENTION_PRICING`, ou entre 7 et 2 557 si le paramètre `--billing-mode` est défini sur `FIXED_RETENTION_PRICING`. Si vous ne le spécifiez pas `--retention-period`, CloudTrail utilise la période de conservation par défaut pour le `--billing-mode`. Si vous créez un magasin de données d'événement d'organisation, incluez le paramètre `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
```

```
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

Vous utiliserez l'ARN (ou le suffixe d'ID de l'ARN) de la réponse comme valeur du paramètre `--event-data-store` à l'étape 3.

3. Exécutez la commande put-insight-selectors pour activer les événements Insights. Les valeurs du sélecteur Insights peuvent être `ApiCallRateInsight`, `ApiErrorRateInsight`, ou les deux. Pour le paramètre `--event-data-store`, spécifiez l'ARN (ou le suffixe d'ID de l'ARN) de l'entrepôt de données d'événement source qui journalise les événements de gestion et activera Insights. Pour le paramètre `--insights-destination`, spécifiez l'ARN (ou le suffixe d'ID de l'ARN) de l'entrepôt de données d'événement de destination qui journalisera les événements Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Le résultat suivant montre le sélecteur d'événements Insights configuré pour l'entrepôt de données d'événement.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Une fois que vous avez activé CloudTrail Insights pour la première fois dans un magasin de données d'événements, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée.

CloudTrail Insights analyse les événements de gestion qui se produisent dans une seule région, et non à l'échelle mondiale. Un événement CloudTrail Insights est généré dans la même région que les événements de gestion connexes.

Dans le cas d'un magasin de données sur les événements d'une organisation, il CloudTrail analyse les événements de gestion du compte de chaque membre au lieu d'analyser l'agrégation de tous les événements de gestion de l'organisation.

Des frais supplémentaires s'appliquent pour l'ingestion d'événements Insights à CloudTrail Lake. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Importez les événements de suivi dans un magasin de données d'événements à l'aide du AWS CLI

Dans le AWS CLI, vous pouvez importer des événements de suivi dans un magasin de données d'événements. La procédure décrite dans cette section explique comment créer et configurer un magasin de données d'événement en exécutant la commande create-event-data-store, puis en important les événements dans ce magasin de données d'événement à l'aide de la commande start-import. Pour plus d'informations sur l'importation d'événements de journal de suivi, y compris des informations sur les considérations et les autorisations requises, consultez Copier des événements de journal de suivi dans un magasin de données d'événement.

Préparation à l'importation d'événements de journal de suivi

Avant d'importer des événements de journal de suivi, effectuez les préparations suivantes.

- Assurez-vous que vous disposez d'un rôle doté des autorisations requises pour importer des événements de journal de suivi dans un magasin de données d'événement.
- Déterminez la valeur --billing-mode que vous souhaitez spécifier pour le magasin de données d'événement. Le paramètre `--billing-mode` détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour le magasin de données d'événement.

Lorsque vous importez des événements de suivi dans CloudTrail Lake, CloudTrail décompressez les journaux stockés au format gzip (compressé). CloudTrail Copie ensuite les événements contenus dans les journaux dans votre banque de données d'événements. La taille des données non compressées peut être supérieure à la taille réelle du stockage Amazon S3. Pour obtenir une estimation générale de la taille des données non compressées, vous pouvez multiplier par 10 la taille des journaux du compartiment S3. Vous pouvez utiliser cette estimation pour choisir la valeur `--billing-mode` correspondant à votre cas d'utilisation.

- Déterminez la valeur que vous souhaitez spécifier pour le paramètre `--retention-period`. CloudTrail ne copiera pas un événement s'il `eventTime` est antérieur à la période de conservation spécifiée.

  Pour déterminer la période de conservation appropriée, faites la somme de l'événement le plus ancien que vous souhaitez copier en jours et du nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événement, comme le montre l'équation suivante :

  Durée de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*

  Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.
- Décidez si vous souhaitez utiliser le magasin de données d'événement pour analyser les événements futurs. Si vous ne souhaitez pas ingérer d'événements futurs, incluez le paramètre `--no-start-ingestion` lorsque vous créez le magasin de données d'événement. Par défaut, le magasin de données d'événement commence à ingérer les événements dès sa création.

Pour créer un magasin de données d'événement et importer des événements de journal de suivi dans celui-ci

1. Exécutez la commande create-event-data-store pour créer le nouveau magasin de données d'événement. Dans cet exemple, le paramètre `--retention-period` est défini sur `120` parce que le plus ancien événement copié date de 90 jours et que nous voulons conserver les événements pendant 30 jours. Le paramètre `--no-start-ingestion` est défini, car nous ne voulons pas ingérer d'événements futurs. Dans cet exemple, le paramètre `--billing-mode` n'a pas été défini, car nous utilisons la valeur par défaut `EXTENDABLE_RETENTION_PRICING` car nous prévoyons d'ingérer moins de 25 To de données d'événement.

> **Note**
>
> Si vous créez le magasin de données d'événement pour remplacer votre journal de suivi, nous vous recommandons de configurer le paramètre `--advanced-event-selectors` pour qu'il corresponde aux sélecteurs d'événements de votre journal de suivi afin de vous assurer que vous bénéficiez de la même couverture d'événement. Par défaut, les magasins de données d'événement journalisent tous les événements de gestion.

```
aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
 120 --no-start-ingestion
```

Voici un exemple de réponse :

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
```

```
}
```

La paramètre initial `Status` est `CREATED` nous allons donc lancer la commande get-event-data-store pour vérifier que l'ingestion est arrêtée.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

La réponse indique que le paramètre `Status` est désormais `STOPPED_INGESTION`, ce qui indique que le magasin de données d'événement n'ingère pas les événements en direct.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. Exécutez la commande start-import pour importer les événements du journal de suivi dans le magasin de données d'événement créé à l'étape 1. Spécifiez l'ARN (ou le suffixe d'ID de l'ARN) du magasin de données d'événement comme valeur du paramètre `--destinations`. Pour le paramètre `--start-event-time`, spécifiez `eventTime` pour l'événement le plus ancien que

vous souhaitez copier et pour le paramètre `--end-event-time`, spécifiez `eventTime` pour l'événement le plus récent que vous souhaitez copier. Pour `--import-source` spécifier l'URI S3 du compartiment S3 contenant vos journaux de suivi, Région AWS celui du compartiment S3 et l'ARN du rôle utilisé pour importer les événements de suivi.

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

Voici un exemple de réponse.

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
   "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
   "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. Exécutez la commande get-import pour obtenir des informations sur l'importation.

```
aws cloudtrail get-import --import-id import-id
```

Voici un exemple de réponse.

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

Une importation se termine par un paramètre `ImportStatus` défini sur `COMPLETED` s'il n'y a pas eu d'échec ou défini sur `FAILED` s'il y a eu des échecs.

Si l'importation est définie sur `FailedEntries`, vous pouvez exécuter la commande list-import-failures pour renvoyer une liste des échecs.

```
aws cloudtrail list-import-failures --import-id import-id
```

Pour réessayer une importation qui a échoué, exécutez la commande start-import avec uniquement le paramètre `--import-id`. Lorsque vous réessayez une importation, elle CloudTrail reprend à l'endroit où l'échec s'est produit.

```
aws cloudtrail start-import --import-id import-id
```

Bénéficiez d'une banque de données sur les événements grâce au AWS CLI

L'exemple de AWS CLI get-event-data-store commande suivant renvoie des informations sur le magasin de données d'événements spécifié par le `--event-data-store` paramètre requis, qui accepte un ARN ou le suffixe d'ID de l'ARN.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Voici un exemple de réponse. Les heures de création et de dernière mise à jour sont au format `timestamp`.

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
```

```
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::bucketName"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

Répertoriez tous les magasins de données d'événements dans un compte auprès du AWS CLI

L'exemple de AWS CLI list-event-data-stores commande suivant renvoie des informations sur tous les magasins de données d'événements d'un compte, dans la région actuelle. Les paramètres facultatifs incluent `--max-results`, pour spécifier un nombre maximal de résultats que la commande doit renvoyer sur une seule page. S'il y a plus de résultats que la valeur `--max-results` spécifiée, exécutez à nouveau la commande en ajoutant la valeur `NextToken` renvoyée pour obtenir la page suivante de résultats.

```
aws cloudtrail list-event-data-stores
```

Voici un exemple de réponse.

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
}
```

Mettez à jour un magasin de données d'événements avec AWS CLI

Les exemples suivants montrent comment mettre à jour un magasin de données d'événement.

Rubriques

- Mettez à jour le mode de facturation avec AWS CLI
- Mettez à jour le mode de rétention, activez la protection contre le licenciement et spécifiez un AWS KMS key avec AWS CLI
- Désactivez la protection contre le licenciement à l'aide du AWS CLI

Mettez à jour le mode de facturation avec AWS CLI

Le paramètre `--billing-mode` pour le magasin de données d'événement détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale du magasin de données d'événement. Si la valeur d'un magasin de données d'événement `--billing-mode` est définie sur `FIXED_RETENTION_PRICING`, vous pouvez modifier la valeur sur `EXTENDABLE_RETENTION_PRICING`. `EXTENDABLE_RETENTION_PRICING` est généralement

recommandé si votre magasin de données d'événement ingère moins de 25 To de données d'événement par mois et si vous souhaitez une période de conservation flexible allant jusqu'à 3 653 jours. Pour plus d'informations sur la tarification, consultez Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

> **Note**
>
> Vous ne pouvez pas remplacer la valeur `--billing-mode EXTENDABLE_RETENTION_PRICING` par `FIXED_RETENTION_PRICING`. Si le mode de facturation du magasin de données d'événement est défini sur `EXTENDABLE_RETENTION_PRICING` et que vous souhaitez utiliser `FIXED_RETENTION_PRICING` à la place, vous pouvez arrêter l'ingestion dans le magasin de données d'événement et créer un nouveau magasin de données d'événement qui utilise `FIXED_RETENTION_PRICING`.

Dans l'exemple de AWS CLI update-event-data-store commande suivant, la `--billing-mode` valeur du magasin de données d'événements passe de `FIXED_RETENTION_PRICING` à`EXTENDABLE_RETENTION_PRICING`. La valeur du paramètre `--event-data-store` requise est un ARN (ou l'ID de suffixe de l'ARN) et est obligatoire ; les autres paramètres sont facultatifs.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
```

```
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Mettez à jour le mode de rétention, activez la protection contre le licenciement et spécifiez un AWS KMS key avec AWS CLI

L'exemple de AWS CLI update-event-data-store commande suivant met à jour un magasin de données d'événements afin de porter sa période de conservation à 100 jours et d'activer la protection contre les résiliations. La valeur du paramètre `--event-data-store` requise est un ARN (ou l'ID de suffixe de l'ARN) et est obligatoire ; les autres paramètres sont facultatifs. Dans cet exemple, le paramètre `--retention-period` est ajouté pour modifier la période de rétention à 100 jours. Vous pouvez éventuellement choisir d'activer le AWS Key Management Service chiffrement et de spécifier un AWS KMS key en ajoutant `--kms-key-id` à la commande et en spécifiant un ARN de clé KMS comme valeur. `--termination-protection-enabled`est ajouté pour activer la protection contre la résiliation sur un magasin de données d'événements pour lequel la protection contre la résiliation n'était pas activée.

Un magasin de données d'événements qui enregistre des événements extérieurs AWS ne peut pas être mis à jour pour enregistrer AWS des événements. De même, un magasin de données d'événements qui enregistre des AWS événements ne peut pas être mis à jour pour enregistrer des événements provenant de l'extérieur AWS.

> **Note**
>
> Si vous réduisez la période de conservation d'une banque de données d'événements, vous CloudTrail supprimerez tous les événements dont la période de conservation est `eventTime` antérieure à la nouvelle. Par exemple, si la période de rétention précédente était de 365 jours

et que vous la réduisez à 100 jours, les événements datant de `eventTime` plus de 100 jours CloudTrail seront supprimés.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Désactivez la protection contre le licenciement à l'aide du AWS CLI

Par défaut, la protection contre la résiliation est activée sur un magasin de données d'événement pour protéger celui-ci contre la suppression accidentelle. Vous ne pouvez pas supprimer un magasin de données d'événement lorsque la protection contre la résiliation est activée. Si vous souhaitez supprimer le magasin de données d'événement, vous devez d'abord désactiver la protection contre la résiliation.

L'exemple de AWS CLI update-event-data-store commande suivant désactive la protection de terminaison en transmettant le `--no-termination-protection-enabled` paramètre.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Arrêtez l'ingestion dans un magasin de données d'événements grâce au AWS CLI

L'exemple de AWS CLI stop-event-data-store-ingestion commande suivant empêche un magasin de données d'événements d'ingérer des événements. Pour arrêter l'ingestion, le `Status` de l'entrepôt de données d'événement doit avoir la valeur `ENABLED` et `eventCategory` doit avoir la valeur `Management`, `Data`, ou `ConfigurationItem`. Me magasin de données d'événement est spécifié par `--event-data-store`, qui accepte un ARN de magasin de données d'événement ou le suffixe d'ID de l'ARN. Après avoir exécuté stop-event-data-store-ingestion, l'état de l'entrepôt de données d'événement passe à `STOPPED_INGESTION`.

L'entrepôt de données d'événement est pris en compte dans le maximum de dix entrepôts de données d'événement de votre compte lorsque son état est `STOPPED_INGESTION`.

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Il n'y a pas de réponse si l'opération est réussie.

Commencez l'ingestion dans un magasin de données d'événements avec le AWS CLI

L'exemple de AWS CLI start-event-data-store-ingestion commande suivant lance l'ingestion d'événements dans un magasin de données d'événements. Pour démarrer l'ingestion, le `Status` de l'entrepôt de données d'événement doit avoir la valeur `STOPPED_INGESTION` et `eventCategory` doit avoir la valeur `Management`, `Data`, ou `ConfigurationItem`. L'entrepôt de données

d'événement est spécifié par `--event-data-store`, qui accepte un ARN d'entrepôt de données d'événement ou le suffixe d'ID de l'ARN. Après avoir exécuté start-event-data-store-ingestion, l'état de l'entrepôt de données d'événement passe à `ENABLED`.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

Il n'y a pas de réponse si l'opération est réussie.

Activer la fédération dans un magasin de données d'événement

Pour activer la fédération, exécutez la commande aws cloudtrail enable-federation en fournissant les paramètres `--event-data-store` et `--role` requis. Pour `--event-data-store`, fournissez l'ARN du magasin de données d'événement (ou le suffixe d'ID de l'ARN). Pour `--role`, fournissez l'ARN correspondant à votre rôle de fédération. Le rôle doit exister dans votre compte et fournir les autorisations minimales requises.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Cet exemple montre comment un administrateur délégué peut activer la fédération sur le magasin de données d'événement d'organisation en spécifiant l'ARN du magasin de données d'événement dans le compte de gestion et l'ARN du rôle de fédération dans le compte administrateur délégué.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-
id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Désactiver la fédération sur un magasin de données d'événement

Pour désactiver la fédération sur le magasin de données d'événement, exécutez la commande aws cloudtrail disable-federation. Le magasin de données d'événement est spécifié par `--event-data-store`, qui accepte un ARN de magasin de données d'événement ou le suffixe d'ID de l'ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> S'il s'agit du magasin de données d'événement d'organisation, vous devez utiliser l'ID du compte de gestion.

Supprimer un magasin de données d'événements à l'aide du AWS CLI

L'exemple de commande AWS CLI delete-event-data-store suivant montre comment désactiver le magasin de données d'événement spécifié par `--event-data-store`, qui accepte un ARN de magasin de données d'événement, ou le suffixe d'ID de l'ARN. Une fois delete-event-data-store exécuté, l'état final du magasin de données d'événement est `PENDING_DELETION`, et le magasin de données d'événement est automatiquement supprimé après une période d'attente de sept jours.

Une fois delete-event-data-store exécuté sur un magasin de données d'événement, vous ne pouvez pas exécuter list-queries, describe-query ou get-query-results sur les requêtes utilisant le magasin de données désactivé. Le magasin de données d'événement est pris en compte dans le nombre maximum de dix magasins de données d'événement de votre compte lorsqu'il est en attente de suppression.

> **Note**
>
> Vous ne pouvez pas supprimer un magasin de données d'événement si `--termination-protection-enabled` est défini ou si le paramètre `FederationStatus` est défini sur `ENABLED`.

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Il n'y a pas de réponse si l'opération est réussie.

Restaurez une banque de données d'événements à l'aide du AWS CLI

L'exemple de commande AWS CLI restore-event-data-store suivant montre comment restaurer un magasin de données d'événement en attente de suppression. Le magasin de données d'événement est spécifié par `--event-data-store`, qui accepte un ARN de magasin de données d'événement

ou le suffixe d'ID de l'ARN. Vous ne pouvez restaurer un magasin de données d'événement supprimé que pendant la période d'attente de sept jours après la suppression.

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

La réponse inclut des informations sur le magasin de données d'événements, y compris son ARN, les sélecteurs d'événement avancés et l'état de la restauration.

Gérer les cycles de vie des magasins de données d'événement

Les étapes du cycle de vie d'un magasin de données d'événement sont les suivantes.

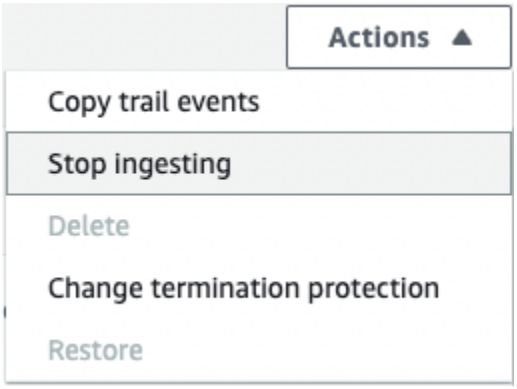
- `CREATED` : état de courte durée indiquant que le magasin de données d'événement a été créé.
- `ENABLED` : l'entrepôt de données d'événement est actif et ingère des événements. Vous pouvez exécuter des requêtes et copier des événements du journal de suivi dans l'entrepôt de données d'événement.
- `STARTING_INGESTION` : état à court terme indiquant que l'entrepôt de données d'événement va commencer à ingérer des événements en direct.
- `STOPPING_INGESTION` : état à court terme indiquant que l'entrepôt de données d'événement cessera d'ingérer des événements en direct.
- `STOPPED_INGESTION` : l'entrepôt de données d'événement n'ingère pas les événements en direct. Vous pouvez toujours exécuter des requêtes sur tous les événements déjà présents dans le magasin de données d'événement et copier les événements du journal de suivi dans le magasin de données d'événement.
- `PENDING_DELETION` : le magasin de données d'événement était dans l'état `ENABLED` ou `STOPPED_INGESTION` et a été supprimé, mais se trouve dans la période d'attente de sept jours précédant la suppression définitive. Vous ne pouvez pas exécuter de requêtes sur le magasin de données d'événement, et aucune opération ne peut être effectuée sur ce dernier, à l'exception de la restauration.

Vous ne pouvez supprimer un magasin de données d'événement que si la fédération et la protection contre la résiliation sont désactivées. La protection contre la résiliation empêche la suppression accidentelle d'un magasin de données d'événement. Par défaut, la protection contre la résiliation est activée sur un magasin de données d'événement. La fédération vous permet d'interroger les données de votre magasin de données d'événement dans Athena et est désactivée par défaut.

Une fois que vous avez supprimé un magasin de données d'événement, il reste dans l'état `PENDING_DELETION` pendant 7 jours avant qu'il ne soit définitivement supprimé. Vous pouvez restaurer un magasin de données d'événement au cours de la période d'attente de sept jours. Lorsqu'il se trouve dans l'état `PENDING_DELETION`, un magasin de données d'événement n'est pas disponible pour les requêtes et aucune autre opération ne peut être effectuée sur le magasin de données d'événement, sauf les opérations de restauration. Un entrepôt de données d'événement en attente de suppression n'ingère pas d'événement et n'entraîne pas de coûts. Toutefois, les magasins de données d'événements en attente de suppression sont pris en compte dans le quota de magasins de données d'événements qui peuvent exister dans un magasin de données d'événements Région AWS.

Actions disponibles dans les entrepôts de données d'événement

Pour supprimer ou restaurer un magasin de données d'événement, copier des journaux de suivi, démarrer ou arrêter l'ingestion d'événements, ou activer ou désactiver la protection contre la résiliation d'un magasin de données d'événement, utilisez les commandes du menu Actions de la page de détails du magasin de données d'événement.



L'option permettant de copier les événements de suivi n'est disponible que sur les magasins de données d'événements contenant des événements CloudTrail de gestion et de données. Les options permettant de démarrer l'ingestion et d'arrêter l'ingestion ne sont disponibles que sur les magasins de données d'événements contenant soit des CloudTrail événements (événements de gestion et de données), soit des éléments AWS Config de configuration.

Copier des événements de journal de suivi dans un magasin de données d'événement

Vous pouvez copier les événements du sentier dans un magasin de données d'événements CloudTrail Lake pour créer un point-in-time instantané des événements enregistrés sur le sentier.

La copie des événements d'un journal de suivi n'interfère pas avec la capacité du journal de suivi à journaliser des événements et ne modifie en aucune façon le journal.

Vous pouvez copier les événements de suivi dans un magasin de données d'événements existant configuré pour les CloudTrail événements, ou vous pouvez créer un nouveau magasin de données d' CloudTrail événements et choisir l'option Copier les événements de suivi dans le cadre de la création du magasin de données d'événements. Pour plus d'informations sur la copie des événements de suivi dans un entrepôt de données d'événement existant, veuillez consulter Copier des événements de journal de suivi dans un magasin de données d'événement existant. Pour plus d'informations sur la création d'un entrepôt de données d'événement, veuillez consulter Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

Si vous copiez des événements de journal de suivi vers le magasin de données d'événement d'une organisation, vous devez utiliser le compte de gestion de l'organisation. Vous ne pouvez pas copier les événements de journal de suivi en utilisant le compte administrateur délégué d'une organisation.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Lorsque vous copiez des événements de parcours dans un magasin de données d'événements CloudTrail Lake, vous êtes facturé en fonction de la quantité de données non compressées ingérée par le magasin de données d'événements.

Lorsque vous copiez des événements de suivi dans CloudTrail Lake, CloudTrail décompressez les journaux stockés au format gzip (compressé), puis copie les événements contenus dans les journaux dans votre magasin de données d'événements. La taille des données non compressées peut être supérieure à la taille réelle du stockage S3. Pour obtenir une estimation générale de la taille des données non compressées, vous pouvez multiplier par 10 la taille des journaux du compartiment S3.

Vous pouvez réduire les coûts en spécifiant une plage de temps plus restreinte pour les événements copiés. Si vous prévoyez de n'utiliser l'entrepôt de données d'événement que pour interroger vos événements copiés, vous pouvez désactiver l'ingestion des événements afin d'éviter d'encourir des frais lors d'événements futurs. Pour plus d'informations, veuillez consulter Tarification AWS CloudTrail et Gestion des coûts CloudTrail du lac.

Scénarios

Le tableau suivant décrit certains scénarios courants de copie d'événements de suivi et explique comment réaliser chaque scénario à l'aide de la console.

Scénario	Comment puis-je y parvenir dans la console ?
Analysez et interrogez les événements historiques des sentiers dans CloudTrail le lac sans ingérer de nouveaux événements	Créez un nouveau magasin de données d'événement et choisissez l'option Copier les événements de suivi dans le cadre de la création du magasin de données d'événement. Lorsque vous créez le magasin de données d'événement, désélectionnez Ingérer les événements (étape 15 de la procédure) pour vous assurer que le magasin de données d'événement ne contient que les événements passés de votre journal de suivi et aucun événement futur.
Remplacez votre parcours existant par un magasin de données sur les événements CloudTrail Lake	Créez un entrepôt de données d'événement avec les mêmes sélecteurs d'événements que votre journal de suivi pour vous assurer que l'entrepôt de données d'événement a la même couverture que votre journal de suivi. Pour éviter de dupliquer les événements entre le journal de suivi source et l'entrepôt de données d'événement de destination, choisissez pour les événements copiés une plage de temps antérieure à la création de l'entrepôt de données d'événement. Une fois l'entrepôt de données d'événement créé, vous pouvez désactiver la journalisation du journal de suivi pour éviter des frais supplémentaires.

Rubriques

Considérations pour copier les événements de journal de suivi

Tenez compte des facteurs suivants lors de la copie d'événements du journal de suivi.

- Lorsque vous copiez des événements de CloudTrail suivi, utilise l'opération d'`GetObject`API S3 pour récupérer les événements de suivi dans le compartiment S3 source. Certaines classes de stockage S3, telles que les niveaux S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts et S3 Intelligent-Tiering Deep Archive ne sont pas accessibles en utilisant `GetObject`. Pour copier les événements de suivi stockés dans ces classes de stockage archivées, vous devez d'abord restaurer une copie à l'aide de l'opération S3 `RestoreObject`. Pour plus d'informations sur la restauration d'objets archivés, veuillez consulter Restauration d'un objet archivé dans le Guide de l'utilisateur Amazon S3.
- Lorsque vous copiez des événements de suivi dans un magasin de données d'événements, CloudTrail copie tous les événements de suivi, quelle que soit la configuration des types d'événements, des sélecteurs d'événements avancés ou Région AWS de la banque de données de destination.
- Avant de copier les événements de suivi dans un magasin de données d'événement existant, assurez-vous que l'option de tarification et la période de conservation du magasin de données d'événement sont configurées de manière appropriée pour votre cas d'utilisation.
  - Option de tarification : l'option de tarification détermine le coût d'ingestion et de stockage des événements. Pour de plus amples informations sur les options de tarification, consultez Tarification d'AWS CloudTrail et Options de tarification du magasin de données d'événement.
  - Période de conservation : La période de conservation détermine la durée pendant laquelle les données d'événements sont conservées dans le magasin de données d'événements. CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.
- Si vous copiez des événements de journal de suivi vers un magasin de données d'événement à des fins d'investigation et que vous ne souhaitez pas ingérer d'événements futurs, vous pouvez arrêter l'ingestion dans le magasin de données d'événement. Lorsque vous créez le magasin de

données d'événement, désélectionnez l'option Ingérer les événements (étape 15 de la procédure) pour vous assurer que le magasin de données d'événement ne contient que les événements passés de votre journal de suivi et aucun événement futur.

- Avant de copier les événements du journal de suivi, désactivez toutes les listes de contrôle d'accès (ACL) associées au compartiment S3 source et mettez à jour la politique du compartiment S3 pour le magasin de données d'événement de destination. Pour plus d'informations sur la mise à jour de la politique de compartiment S3, veuillez consulter Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi. Pour plus d'informations, veuillez consulter Contrôle de la propriété des objets et désactivation des listes ACL pour votre compartiment dans le Guide de l'utilisateur Amazon S3.
- CloudTrail copie uniquement les événements de suivi à partir des fichiers journaux compressés Gzip qui se trouvent dans le compartiment S3 source. CloudTrail ne copie pas les événements de suivi à partir de fichiers journaux non compressés ou de fichiers journaux compressés dans un format autre que Gzip.
- Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez pour les événements copiés une plage de temps antérieure à la création du magasin de données d'événement.
- Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, vous devez choisir le préfixe lorsque vous copiez des événements de suivi.
- Pour copier les événements de journal de suivi vers le magasin de données d'événement d'une organisation, vous devez utiliser le compte de gestion de l'organisation. Le compte d'administrateur délégué ne peut pas copier les événements de journal de suivi vers le magasin de données d'événement d'une organisation.

Autorisations requises pour copier les événements de journal de suivi

Avant de copier des événements de suivi, assurez-vous de disposer de toutes les autorisations requises pour votre rôle IAM. Vous devez uniquement mettre à jour les autorisations du rôle IAM si vous choisissez un rôle IAM existant pour copier les événements de journal de suivi. Si vous choisissez de créer un nouveau rôle IAM, CloudTrail fournit toutes les autorisations nécessaires pour ce rôle.

Si le compartiment S3 source utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique de clé KMS autorise CloudTrail le déchiffrement des données du compartiment. Si le compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé CloudTrail pour autoriser le déchiffrement des données du compartiment.

Rubriques

- Autorisations IAM pour copier les événements de journal de suivi
- Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi
- Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source

Autorisations IAM pour copier les événements de journal de suivi

Lorsque vous copiez des événements de journal de suivi, vous pouvez créer un nouveau rôle IAM ou utiliser un rôle IAM existant. Lorsque vous choisissez un nouveau rôle IAM, vous CloudTrail créez un rôle IAM avec les autorisations requises et aucune autre action n'est requise de votre part.

Si vous choisissez un rôle existant, assurez-vous que les politiques du rôle IAM autorisent la copie CloudTrail des événements de suivi depuis le compartiment S3 source. Cette section fournit des exemples de politiques d'approbation et d'autorisation requises du rôle IAM.

L'exemple suivant fournit la politique d'autorisation, qui permet CloudTrail de copier les événements de suivi depuis le compartiment S3 source. Remplacez *myBucketNameMyAccountId*, *region*, *prefix* et *eventDataStoreId* par les valeurs appropriées à votre configuration. Le *MyAccountID* est l'ID de AWS compte utilisé pour CloudTrail Lake, qui peut être différent de l'ID de AWS compte du compartiment S3.

Remplacez *key-region*, *keyAccountID* et *keyID* par les valeurs de la clé KMS utilisée pour chiffrer le compartiment S3 source. Vous pouvez omettre l'instruction `AWSCloudTrailImportKeyAccess` si le compartiment S3 source n'utilise pas de clé KMS pour le chiffrement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
```

```
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

L'exemple suivant fournit la politique de confiance IAM, qui permet d' CloudTrail assumer un rôle IAM pour copier les événements de suivi depuis le compartiment S3 source. Remplacez *MyAccountId*, *region* et *eventDataStoreArn par* les valeurs appropriées à votre configuration. Le *MyAccountID* est l' Compte AWS ID utilisé pour CloudTrail Lake, qui peut être différent de l'ID de AWS compte pour le compartiment S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi

Par défaut, les objets et les compartiments Amazon S3 sont privés. Seul le propriétaire de la ressource (le compte AWS qui a créé le compartiment) peut accéder au compartiment et aux objets qu'il contient. Le propriétaire de la ressource peut accorder des autorisations d'accès à d'autres ressources et à d'autres utilisateurs en créant une stratégie d'accès.

Avant de copier les événements de suivi, vous devez mettre à jour la politique du compartiment S3 CloudTrail pour autoriser la copie des événements de suivi depuis le compartiment S3 source.

Vous pouvez ajouter l'instruction suivante à la politique du compartiment S3 pour accorder ces autorisations. Remplacez *roLearn* et *myBucketName*par les valeurs appropriées à votre configuration.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
```

```
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source

Si le compartiment S3 source utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique de clé KMS fournit CloudTrail les `kms:GenerateDataKey` autorisations `kms:Decrypt` et les autorisations nécessaires pour copier les événements de suivi depuis un compartiment S3 avec le chiffrement SSE-KMS activé. Si votre compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la stratégie de chaque clé. La mise à jour de la politique des clés KMS permet CloudTrail de déchiffrer les données dans le compartiment S3 source, d'exécuter des contrôles de validation pour s'assurer que les événements sont conformes aux CloudTrail normes et de copier les événements dans le magasin de données d'événements CloudTrail Lake.

L'exemple suivant fournit la politique de clé KMS, qui permet CloudTrail de déchiffrer les données dans le compartiment S3 source. Remplacez *roLearn myBucketName*, *MyAccountId*, *region* et *eventDataStoreId* par les valeurs appropriées à votre configuration. Le *MyAccountID* est l'ID de AWS compte utilisé pour CloudTrail Lake, qui peut être différent de l'ID de AWS compte du compartiment S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
```

```
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Copier des événements de journal de suivi dans un magasin de données d'événement existant

Utilisez la procédure suivante pour copier les événements du journal de suivi vers un magasin de données d'événement existant. Pour plus d'informations sur la création d'un nouveau magasin de données d'événement, veuillez consulter Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

> **Note**
>
> Avant de copier les événements de suivi dans un magasin de données d'événement existant, assurez-vous que l'option de tarification et la période de conservation du magasin de données d'événement sont configurées de manière appropriée pour votre cas d'utilisation.
>
> - Option de tarification : l'option de tarification détermine le coût d'ingestion et de stockage des événements. Pour de plus amples informations sur les options de tarification, consultez Tarification d'AWS CloudTrail et Options de tarification du magasin de données d'événement.
> - Période de conservation : La période de conservation détermine la durée pendant laquelle les données d'événements sont conservées dans le magasin de données d'événements. CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et

que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.

Pour copier des événements de journal de suivi dans un magasin de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Copier les événements de suivi.
4. Sur la page Copy trail events(Copier les événements de suivi), pour Event source (Origine de l'événement), choisissez le journal de suivi que vous souhaitez copier. Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, choisissez Enter S3 URI, puis Browse S3 pour accéder au préfixe. Si le compartiment S3 source pour le suivi utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique en matière de clés KMS autorise CloudTrail le déchiffrement des données. Si votre compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé afin de CloudTrail permettre le déchiffrement des données du compartiment. Pour plus d'informations sur la mise à jour de la stratégie de clé KMS, veuillez consulter Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source.

   La politique du compartiment S3 doit autoriser CloudTrail l'accès à la copie des événements de suivi depuis votre compartiment S3. Pour plus d'informations sur la mise à jour de la politique de compartiment S3, veuillez consulter Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi.
5. Pour Spécifier une plage temporelle d'événements, choisissez la plage de temps pour copier les événements. CloudTrail vérifie le préfixe et le nom du fichier journal pour vérifier que le nom contient une date comprise entre les dates de début et de fin choisies avant de tenter de copier les événements de suivi. Vous avez le choix entre Plage relative ou Plage absolue. Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez une plage de temps antérieure à la création du magasin de données d'événement.

> **Note**
>
> CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Par exemple, si la période de conservation d'un magasin de données d'événements est de 90 jours, aucun événement de suivi datant de `eventTime` plus de 90 jours ne CloudTrail sera copié.

- Si vous choisissez Plage relative, vous pouvez choisir de copier les événements enregistrés au cours des 6 derniers mois, 1 an, 2 ans, 7 ans ou une plage personnalisée. CloudTrail copie les événements enregistrés pendant la période choisie.
- Si vous choisissez la plage absolue, vous pouvez choisir une date de début et une date de fin spécifiques. CloudTrail copie les événements survenus entre les dates de début et de fin choisies.

6. Pour Lieu de diffusion, sélectionnez le magasin de données d'événement de destination dans la liste déroulante.
7. Pour Autorisations, sélectionnez l'une des options de rôle IAM suivantes. Si vous choisissez un rôle IAM existant, vérifiez que la politique de rôle IAM fournit les autorisations nécessaires. Pour plus d'informations sur la mise à jour des autorisations du rôle IAM, consultez Autorisations IAM pour copier les événements de journal de suivi.

   - Sélectionnez Créer un nouveau rôle (recommandé) pour créer un nouveau rôle IAM. Pour Enter IAM role name (Saisir le nom du rôle IAM), saisissez un nom pour le rôle. CloudTrail crée automatiquement les autorisations nécessaires pour ce nouveau rôle.
   - Choisissez Utiliser un ARN de rôle IAM personnalisé pour utiliser un rôle IAM personnalisé qui n'est pas répertorié. Pour Enter IAM role ARN (Saisir l'ARN du rôle IAM), saisissez l'ARN IAM.
   - Choisissez un rôle IAM existant dans la liste déroulante.
8. Choisissez Copy events (Copier les événements).
9. Une confirmation vous est demandée. Dès que vous souhaitez confirmer, sélectionnez Copy trail events to Lake (Copier les événements du journal de suivi sur Lake), puis Copy events (Copier les événements).
10. Sur la page Copy details (Copier les détails), vous pouvez consulter le statut de la copie et les échecs éventuels. Lorsque la copie d'un événement de journal de suivi est terminée, son Copy

status (Statut de la copie) est défini sur Completed (Terminé) si aucune erreur n'est survenue, ou Failed (Échec) si des erreurs sont survenues.

> **Note**
>
> Les détails affichés sur la page des détails de la copie d'événement ne sont pas en temps réel. Les valeurs réelles des détails tels que les Prefixes copied (Préfixes copiés) peuvent être plus élevées que ce qui est indiqué sur la page. CloudTrail met à jour les détails progressivement au cours de la copie de l'événement.

11. Si le Statut de la copie est Échec, corrigez les erreurs qui s'affichent dans Échecs de la copie, puis sélectionnez Réessayer la copie. Lorsque vous réessayez d'effectuer une copie, elle CloudTrail reprend à l'endroit où l'échec s'est produit.

Pour plus d'informations sur l'affichage des informations relatives à la copie d'un événement de journal de suivi, veuillez consulter Informations de copie d'événement.

Informations de copie d'événement

Après le démarrage de la copie d'un événement de journal de suivi, vous pouvez consulter les informations relatives à la copie d'événement, y compris son statut et les informations concernant les échecs éventuels.

> **Note**
>
> Les détails affichés sur la page des détails de la copie d'événement ne sont pas en temps réel. Les valeurs réelles des détails tels que les Prefixes copied (Préfixes copiés) peuvent être plus élevées que ce qui est indiqué sur la page. CloudTrail met à jour les détails progressivement au cours de la copie de l'événement.

Pour accéder à la page de détails de la copie d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation de gauche, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez le magasin de données d'événement.

4. Choisissez la copie d'événement dans la section Event copy status (État de la copie d'événement).

Informations relatives à la copie

Dans Copy details (Informations relatives à la copie), vous pouvez afficher les informations suivantes concernant la copie d'événement de journal de suivi.

- Emplacement S3 du journal des événements : l'emplacement du compartiment S3 source contenant les fichiers journaux des événements de journal de suivi.
- ID de copie : l'identifiant de la copie.
- Préfixes copiés : représente le nombre de préfixes S3 copiés. Lors de la copie d'un événement de suivi, CloudTrail copie les événements dans les fichiers journaux de suivi enregistrés dans les préfixes.
- Statut de la copie : le statut de la copie.
  - Initialisation : statut initial affiché lorsque la copie de l'événement de journal de suivi commence.
  - En cours : indique que la copie de l'événement de journal de suivi est en cours.

    > **Note**
    >
    > Vous ne pouvez pas copier les événements du journal de suivi si une autre copie de ces événements est En cours. Pour interrompre la copie d'un événement de journal de suivi, sélectionnez Stop copy (Interrompre la copie).

  - Interrompu : indique qu'une action Stop copy (Interrompre la copie) s'est produite. Pour réessayer de copier un événement de journal de suivi, sélectionnez Retry copy (Réessayer la copie).
  - Échec : la copie est terminée, mais certains événements de journal de suivi n'ont pas pu être copiés. Consultez les messages d'erreur dans Copy failures (Échecs de la copie). Pour réessayer de copier un événement de journal de suivi, sélectionnez Retry copy (Réessayer la copie). Lorsque vous réessayez d'effectuer une copie, elle CloudTrail reprend à l'endroit où l'échec s'est produit.
  - Terminé : la copie s'est terminée sans erreur. Vous pouvez interroger les événements de journal de suivi copiés dans le magasin de données d'événement.
- Heure de création : indique quand la copie de l'événement de journal de suivi a commencé.

- Heure de fin : indique quand la copie de l'événement de journal de suivi s'est terminée ou interrompue.

Échecs de la copie

Dans Copy failures (Échecs de la copie), vous pouvez consulter l'emplacement, le message et le type d'erreur pour chaque échec de copie. Les causes d'échec les plus courantes incluent le fait qu'un préfixe S3 contenait un fichier non compressé ou un fichier fourni par un service autre que. CloudTrail Une autre cause possible d'échec concerne les problèmes d'accès. Par exemple, si le compartiment S3 du magasin de données d'événements n'autorisait pas l' CloudTrail accès à l'importation des événements, une `AccessDenied` erreur s'afficherait.

Pour chaque échec de copie, consultez les informations d'erreur suivantes.

- L'emplacement de l'erreur : indique l'emplacement où l'erreur s'est produite dans le compartiment S3. Si une erreur se produisait parce que le compartiment S3 source contenait un fichier non compressé, l'emplacement de l'erreur inclurait le préfixe où se trouverait ce fichier.
- Le message d'erreur : fournit une explication quant à la survenue de l'erreur.
- Le type d'erreur : indique le type d'erreur. Par exemple, un type d'erreur `AccessDenied` indique que l'erreur est survenue en raison d'un problème d'autorisations. Pour plus d'informations sur les autorisations requises pour copier des événements de journal de suivi, veuillez consulter Autorisations requises pour copier les événements de journal de suivi.

Après avoir résolu tous les problèmes, sélectionnez Retry copy (Réessayer la copie). Lorsque vous réessayez d'effectuer une copie, elle CloudTrail reprend à l'endroit où l'échec s'est produit.

Exemple : copier les événements de suivi dans un nouveau magasin de données d'événements

Cette procédure pas à pas vous explique comment copier des événements de parcours dans un nouveau magasin de données d'événements CloudTrail Lake à des fins d'analyse historique. Pour plus d'informations sur la copie d'événements de journal de suivi, veuillez consulter Copier des événements de journal de suivi dans un magasin de données d'événement.

Pour copier des événements de journal de suivi dans un entrepôt de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.

2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.
3. Choisissez Créer un magasin de données d'événement.
4. Sur la page Configurer le magasin de données d'événements, dans Détails généraux, donnez un nom à votre magasin de données d'événements, tel que *my-management-events-eds*. Comme bonne pratique, utilisez un nom qui identifie rapidement l'objectif de l'entrepôt de données d'événement. Pour plus d'informations sur les exigences en matière de CloudTrail dénomination, consultezExigences de dénomination.
5. Choisissez l'option de tarification que vous souhaitez utiliser pour votre magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que la période de conservation par défaut et maximale pour votre magasin de données d'événement. Pour plus d'informations, veuillez consulter Tarification d'AWS CloudTrail et Gestion des coûts CloudTrail du lac.

   Les options suivantes sont disponibles :

   - Tarif de rétention extensible d'un an : généralement recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut.
     - Période de conservation par défaut : 366 jours.
     - Période de conservation maximale : 3 653 jours
   - Tarif de rétention sur sept ans : recommandé si vous prévoyez d'ingérer plus de 25 To de données d'événement par mois et que vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires.
     - Période de conservation par défaut : 2 557 jours.
     - Période de conservation maximale : 2 557 jours
6. Spécifiez une période de conservation pour le magasin de données d'événement. Les périodes de conservation peuvent être comprises entre 7 jours et 3 653 jours (environ 10 ans) pour l'option de tarification de rétention extensible d'un an, ou entre 7 jours et 2 557 jours (environ sept ans) pour l'option de tarification de rétention sur sept ans.

   CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si celui-ci se situe dans la période de conservation spécifiée. `eventTime` Par exemple, si vous spécifiez

une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsqu'ils datent `eventTime` de plus de 90 jours.

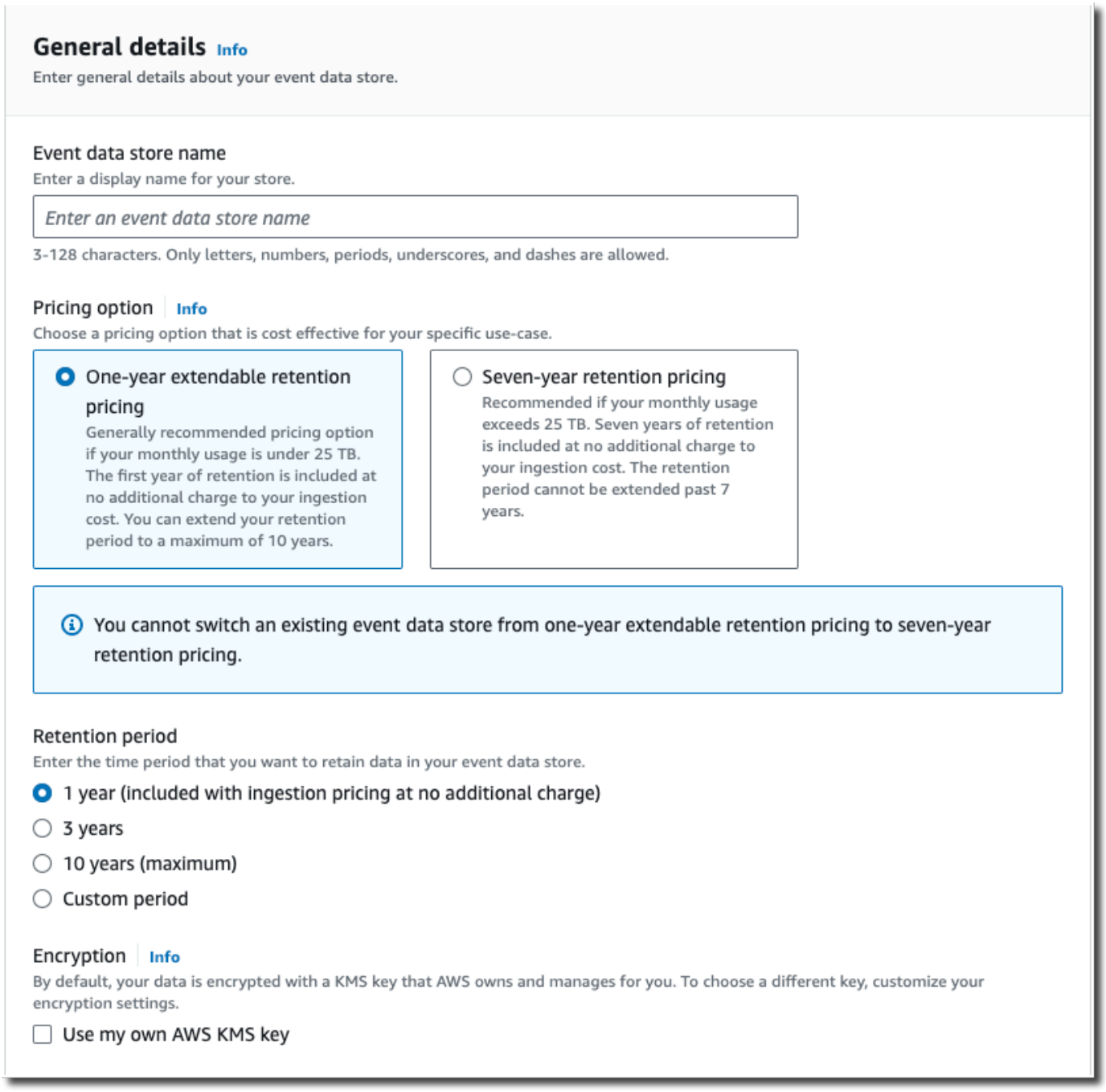
> **Note**
>
> CloudTrail ne copiera pas un événement s'il `eventTime` est antérieur à la période de conservation spécifiée.
> Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.

7. (Facultatif) Dans Chiffrement, indiquez si vous souhaitez chiffrer l'entrepôt de données d'événement à l'aide de votre propre clé KMS. Par défaut, tous les événements d'un magasin de données d'événements sont chiffrés à CloudTrail l'aide d'une clé KMS qui vous AWS appartient et qui la gère pour vous.

   Pour activer le chiffrement à l'aide de votre propre clé KMS, choisissez Utiliser ma propre AWS KMS key. Choisissez Nouveau pour en AWS KMS key créer une pour vous, ou choisissez Existant pour utiliser une clé KMS existante. Dans Enter KMS alias, spécifiez un alias au format `alias/` *`MyAliasName`*. L'utilisation de votre propre clé KMS nécessite que vous modifiiez votre politique de clé KMS pour autoriser le chiffrement et le déchiffrement des CloudTrail journaux. Pour plus d'informations, consultezConfigurer les politiques AWS KMS clés pour CloudTrail. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

   L'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée.

> **Note**
>
> Pour activer AWS Key Management Service le chiffrement pour le magasin de données d'événements d'une organisation, vous devez utiliser une clé KMS existante pour le compte de gestion.



8. (Facultatif) Si vous souhaitez interroger les données de votre événement à l'aide d'Amazon Athena, choisissez Activer dans Fédération de requêtes Lake. La fédération vous permet de visualiser les métadonnées associées au magasin de données d'événement dans le catalogue de données d' AWS Glue et d'exécuter des requêtes SQL sur les données d'événement dans Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.

   Pour activer la fédération de requêtes Lake, choisissez Activer, puis procédez comme suit :

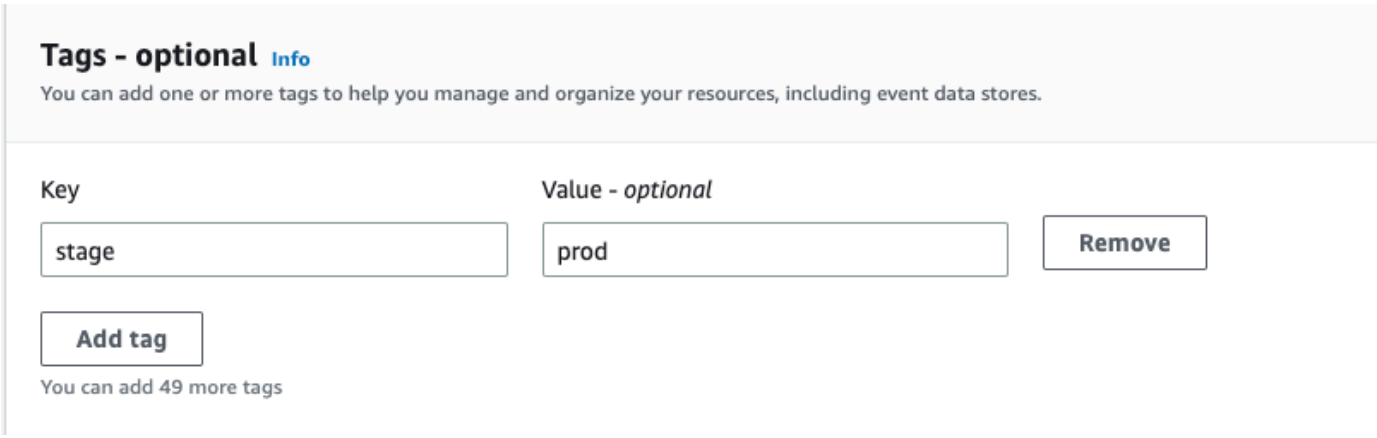
   a. Choisissez si vous souhaitez créer un rôle ou utiliser un rôle IAM existant. AWS Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous choisissez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.

   b. Si vous créez un rôle, saisissez un nom pour identifier le rôle.

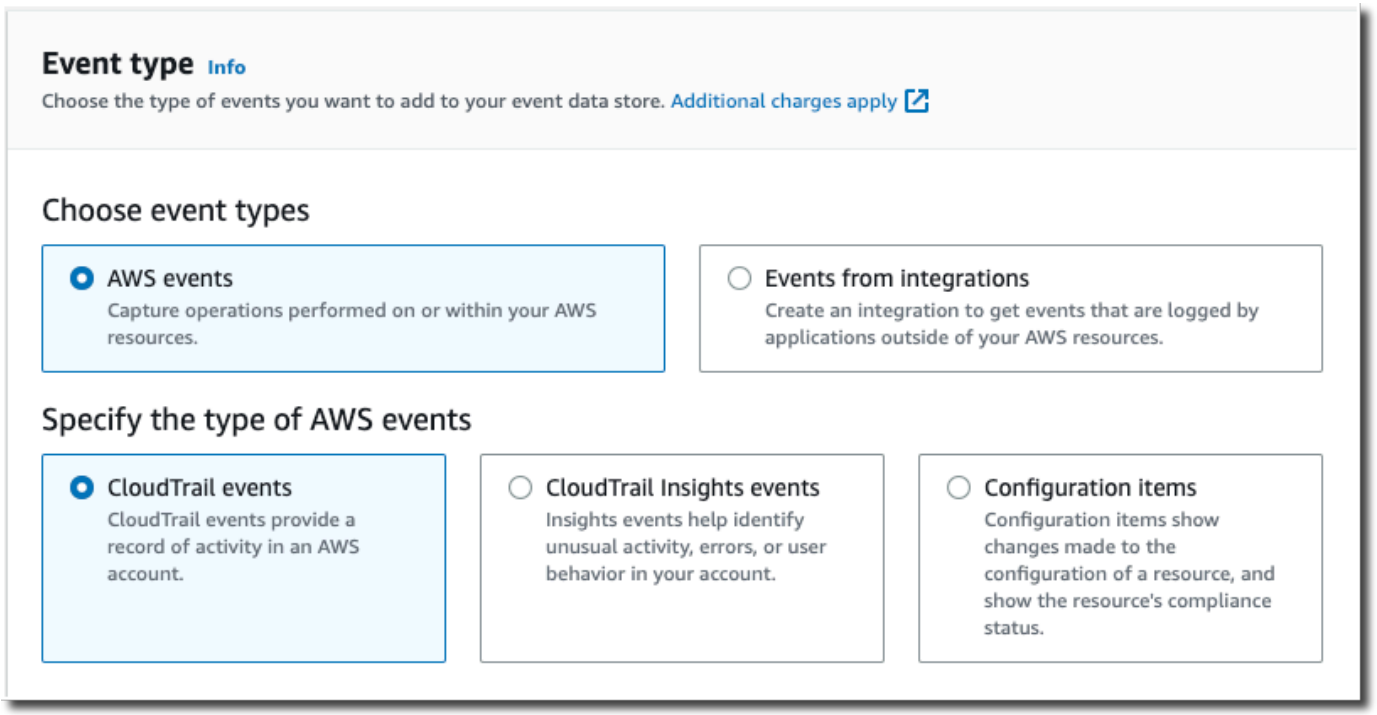
   c. Si vous utilisez un rôle existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.

9. (Facultatif) Dans Balises, ajoutez une ou plusieurs identifications personnalisées (paires valeur-clé) à votre magasin de données d'événement. Les balises peuvent vous aider à identifier les magasins de données de vos CloudTrail événements. Par exemple, il est possible d'attacher une balise portant le nom **`stage`** à la valeur **`prod`**. Vous pouvez utiliser des balises pour limiter l'accès à votre entrepôt de données d'événement. Vous pouvez également utiliser des balises pour suivre les coûts de requête et d'ingestion pour votre entrepôt de données d'événement.

   Pour plus d'informations sur l'utilisation des balises pour le suivi des coûts, veuillez consulter Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un entrepôt de données d'événement basé sur des balises, veuillez consulter Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises AWS, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

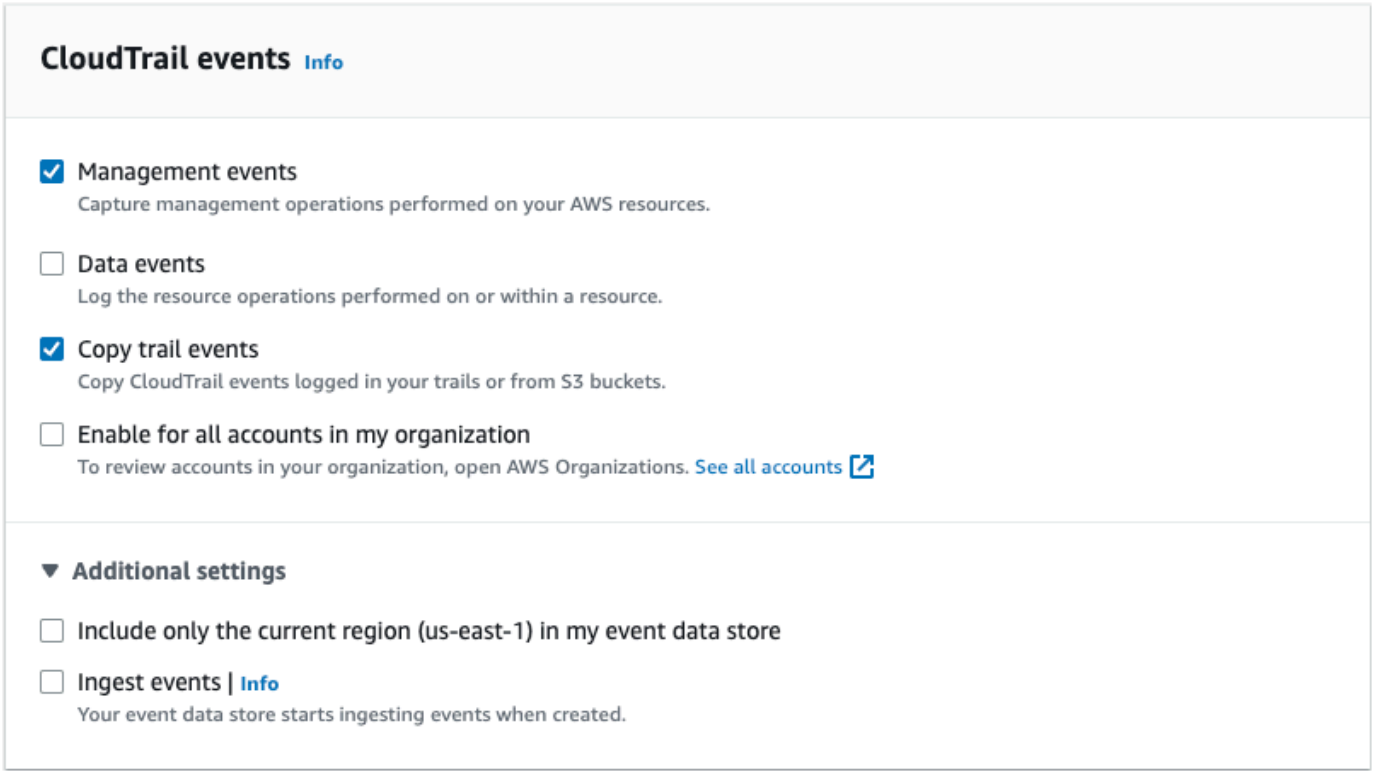


10. Choisissez Suivant pour configurer le magasin de données d'événement.
11. Sur la page Choisir des événements, conservez les sélections par défaut pour Type d'événement.



12. Pour les CloudTrail événements, nous laisserons les événements de gestion sélectionnés et choisirons Copier les événements de piste. Dans cet exemple, les types d'événements ne nous intéressent pas, car nous n'utilisons l'entrepôt de données d'événement que pour analyser les événements passés et non pour ingérer les événements futurs.

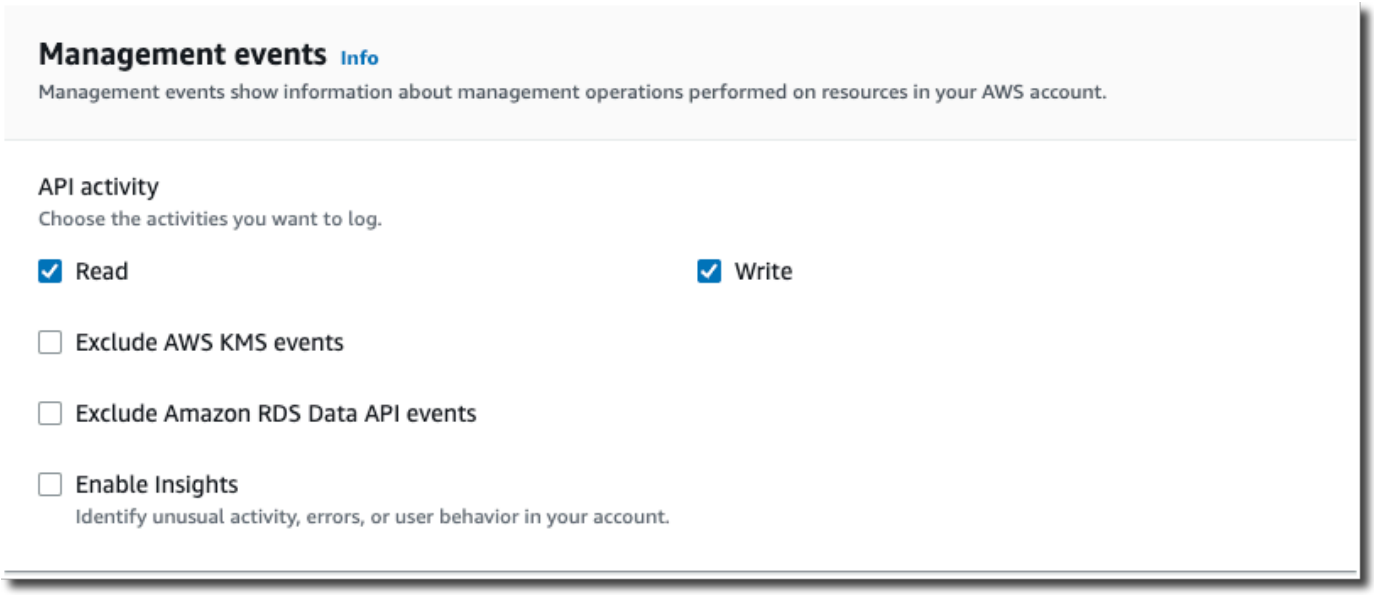
    Si vous créez un entrepôt de données d'événement pour remplacer un journal de suivi existant, choisissez les mêmes sélecteurs d'événements que votre journal de suivi pour vous assurer que l'entrepôt de données d'événement couvre les mêmes événements.



13. Choisissez Activer pour tous les comptes de mon organisation s'il s'agit d'un entrepôt de données d'événement d'organisation. Cette option ne pourra pas être modifiée à moins que vous ayez des comptes configurés dans AWS Organizations.

> **Note**
>
> Si vous créez un entrepôt de données d'événement d'organisation, vous devez être connecté avec le compte de gestion de l'organisation, car seul celui-ci peut copier les événements de journal de suivi vers l'entrepôt de données d'événement d'organisation.

14. Pour Paramètres supplémentaires, nous allons désélectionner Ingérer les événements, car dans cet exemple, nous ne voulons pas que l'entrepôt de données d'événement ingère des événements futurs, puisque nous ne sommes intéressés que par l'interrogation des événements copiés. Par défaut, un magasin de données d'événements collecte les événements pour tous Régions AWS et commence à les ingérer dès sa création.
15. Pour Événements de gestion, nous conserverons les paramètres par défaut.



16. Dans la zone Copier les événements du journal de suivi, effectuez les étapes suivantes.

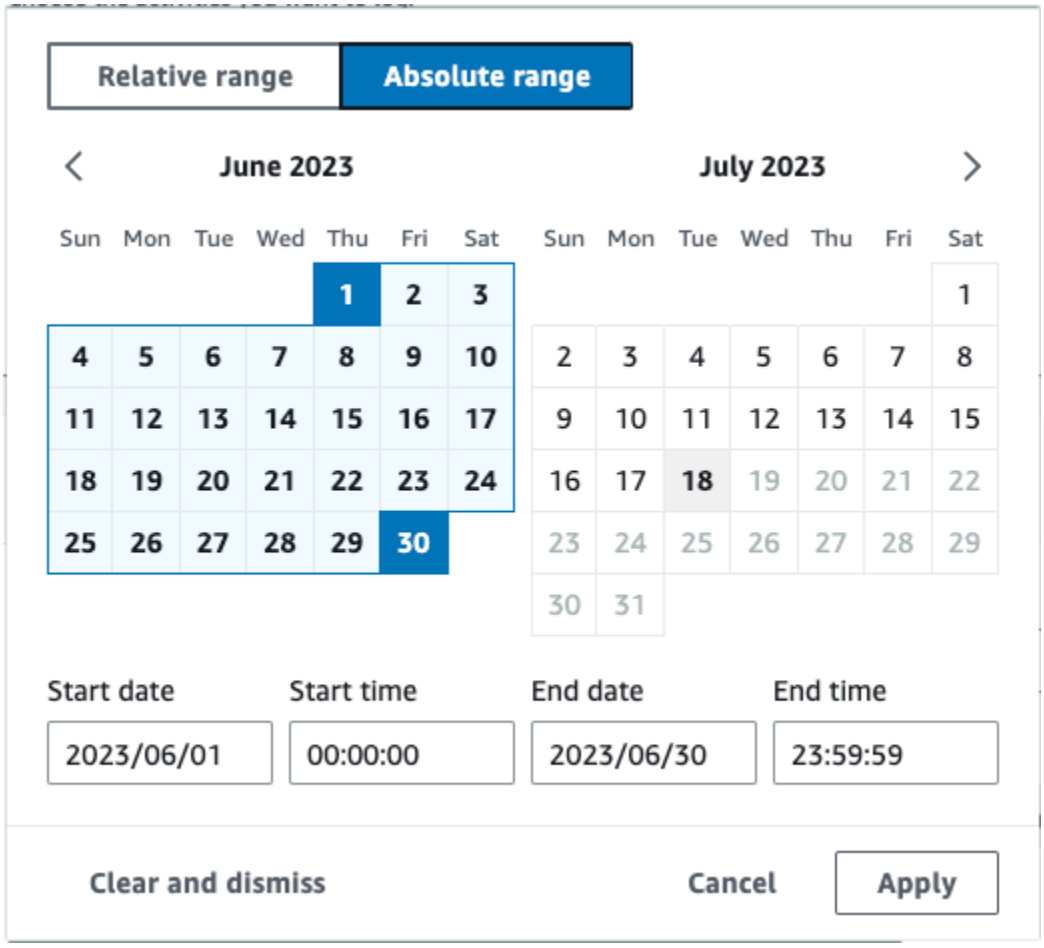
    a. Sélectionnez le journal de suivi que vous voulez copier. Dans cet exemple, nous allons choisir un journal de suivi nommé *`management-events`*.

       Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, choisissez Enter S3 URI, puis Browse S3 pour accéder au préfixe. Si le compartiment S3 source pour le suivi utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique en matière de clés KMS autorise CloudTrail le déchiffrement des données. Si votre compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé afin de CloudTrail permettre le déchiffrement des données du compartiment. Pour plus d'informations sur la mise à jour de la stratégie de clé KMS, veuillez consulter Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source.

    b. Choisissez un intervalle de temps pour copier les événements. CloudTrail vérifie le préfixe et le nom du fichier journal pour vérifier que le nom contient une date comprise entre les dates de début et de fin choisies avant de tenter de copier les événements de suivi. Vous avez le choix entre Plage relative ou Plage absolue. Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez une plage de temps antérieure à la création du magasin de données d'événement.

- Si vous choisissez Plage relative, vous pouvez choisir de copier les événements enregistrés au cours des 6 derniers mois, 1 an, 2 ans, 7 ans ou une plage personnalisée. CloudTrail copie les événements enregistrés pendant la période choisie.
- Si vous choisissez la plage absolue, vous pouvez choisir une date de début et une date de fin spécifiques. CloudTrail copie les événements survenus entre les dates de début et de fin choisies.

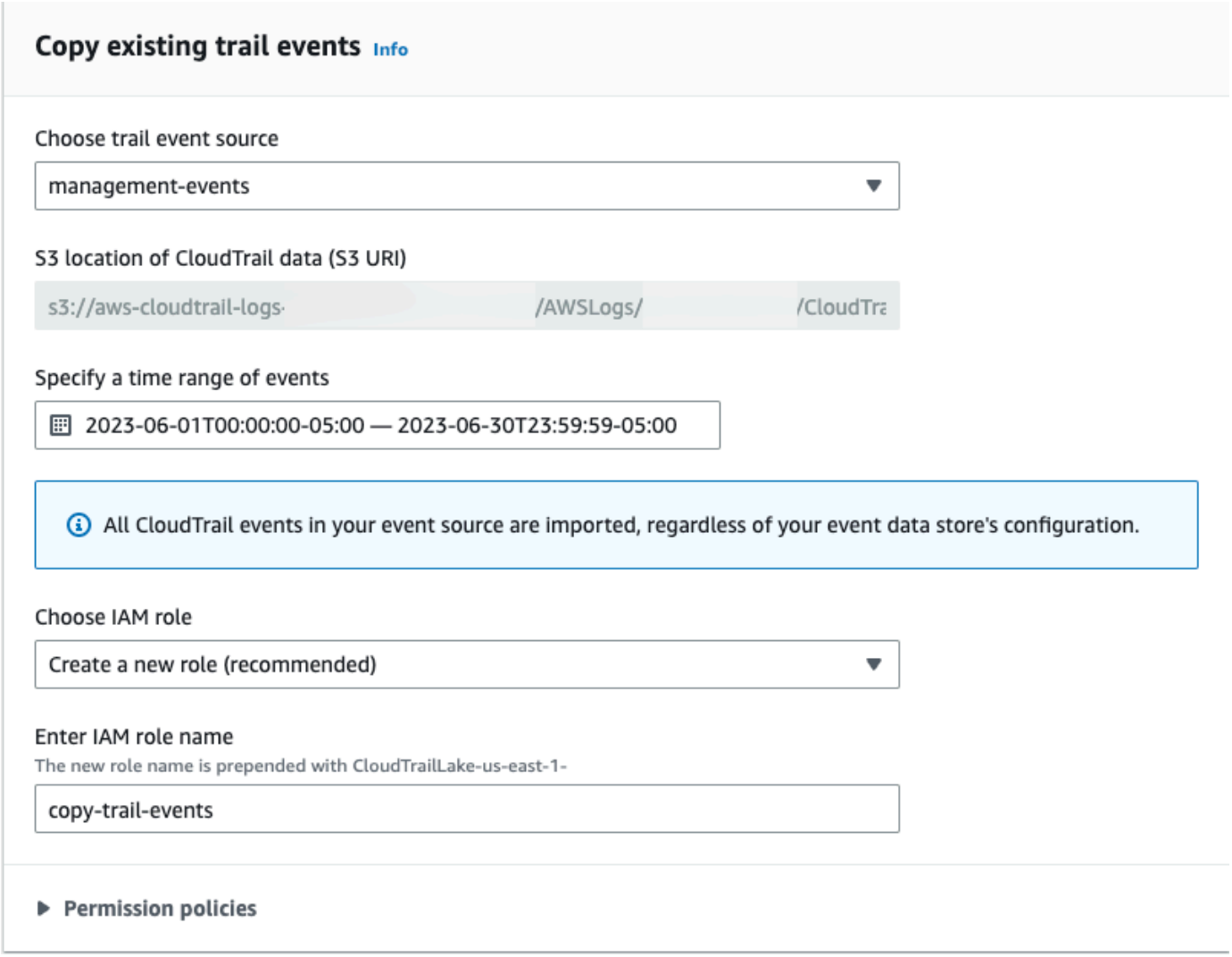
Dans cet exemple, nous allons choisir Plage absolue et nous allons sélectionner l'ensemble du mois de juin.



c. Pour Autorisations, sélectionnez l'une des options de rôle IAM suivantes. Si vous choisissez un rôle IAM existant, vérifiez que la politique de rôle IAM fournit les autorisations nécessaires. Pour plus d'informations sur la mise à jour des autorisations du rôle IAM, consultez Autorisations IAM pour copier les événements de journal de suivi.

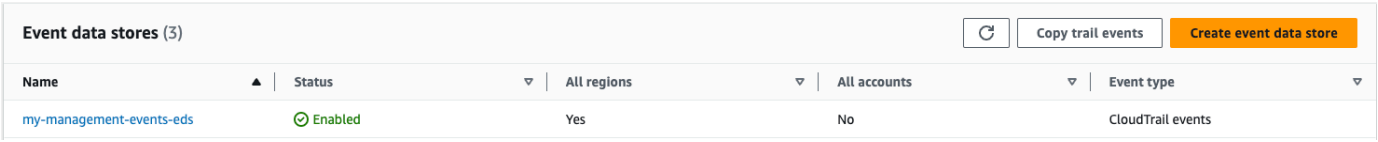
- Sélectionnez Créer un nouveau rôle (recommandé) pour créer un nouveau rôle IAM. Pour Enter IAM role name, saisissez le nom du rôle. CloudTrail crée automatiquement les autorisations nécessaires pour ce nouveau rôle.
- Choisissez Utiliser un ARN de rôle IAM personnalisé pour utiliser un rôle IAM personnalisé qui n'est pas répertorié. Pour Enter IAM role ARN (Saisir l'ARN du rôle IAM), saisissez l'ARN IAM.
- Choisissez un rôle IAM existant dans la liste déroulante.

Dans cet exemple, nous choisirons Créer un nouveau rôle (recommandé) et nous fournirons le nom **`copy-trail-events`**.



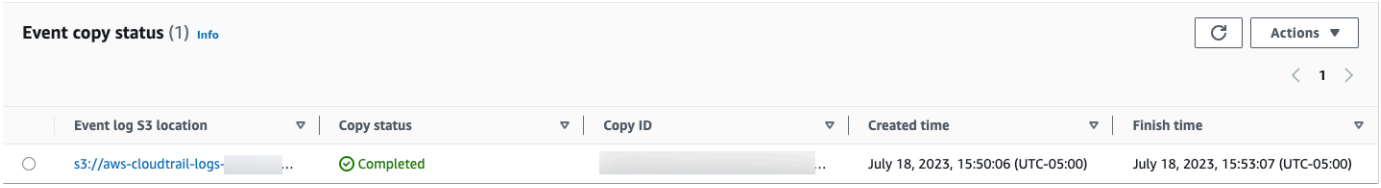
17. Choisissez Suivant pour examiner vos préférences.

18. Sur la page Review and create (Vérifier et créer), examinez vos choix. Choisissez Modifier (Edit) pour apporter des modifications à la section. Lorsque vous êtes prêt à créer le magasin de données d'événement, choisissez Créer un magasin de données d'événement.
19. Le nouvel entrepôt de données d'événement est visible dans la table Entrepôts de données d'événement sur la page Entrepôts de données d'événement.

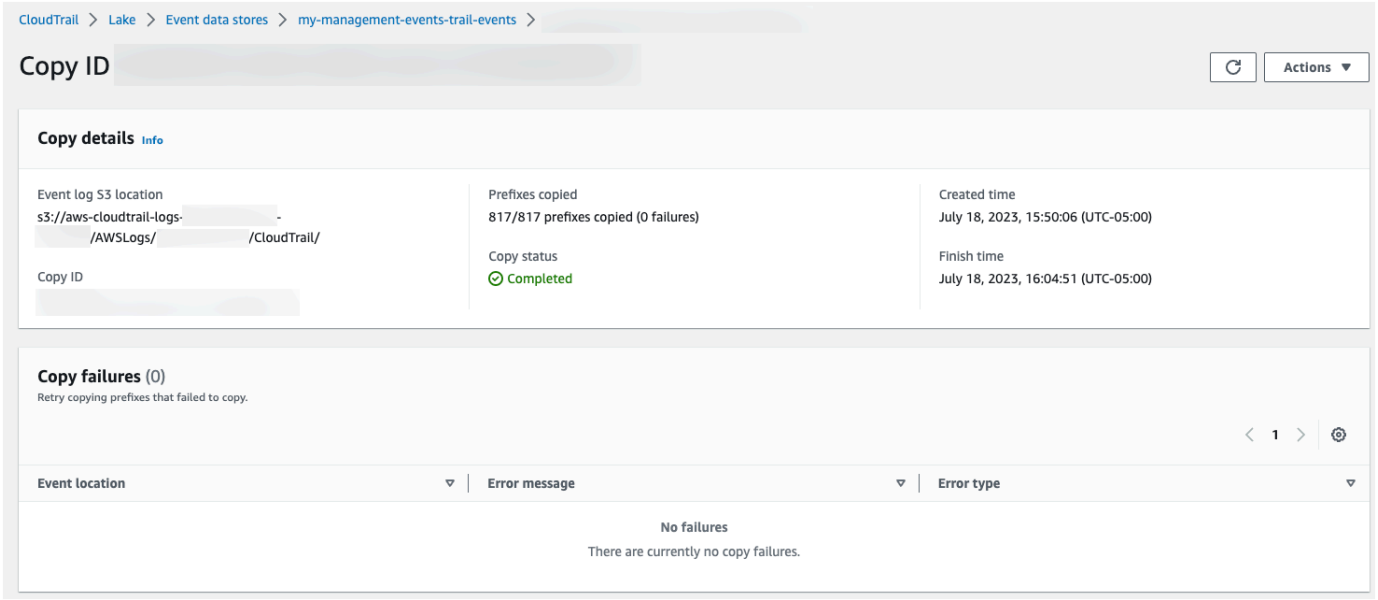


20. Choisissez le nom de l'entrepôt de données d'événement pour afficher la page contenant ses détails. La page de détails indique les détails de votre entrepôt de données d'événement et le statut de la copie. L'état de la copie d'événement est affiché dans la zone État de la copie d'événement.

    Lorsque la copie d'un événement de journal de suivi est terminée, son Statut de la copie est défini sur Terminé si aucune erreur n'est survenue, ou Échec si des erreurs sont survenues.



21. Pour afficher plus de détails sur la copie, choisissez le nom de la copie dans la colonne Emplacement S3 du journal des événements ou choisissez l'option Afficher les détails dans le menu Actions. Pour plus d'informations sur l'affichage des informations relatives à la copie d'un événement de journal de suivi, veuillez consulter Informations de copie d'événement.



22. La zone Échecs de copie indique toutes les erreurs survenues lors de la copie des événements de suivi. Si le Statut de la copie est Échec, corrigez les erreurs qui s'affichent dans Échecs de la copie, puis sélectionnez Réessayer la copie. Lorsque vous réessayez d'effectuer une copie, elle CloudTrail reprend à l'endroit où l'échec s'est produit.

Fédérer un magasin de données d'événement

La fédération d'un magasin de données d'événements vous permet de consulter les métadonnées associées au magasin de données d'événements dans le catalogue de AWS Glue données, d'enregistrer le catalogue de données auprès de celui-ci AWS Lake Formation et d'exécuter des requêtes SQL sur les données de vos événements à l'aide d'Amazon Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger.

Vous pouvez activer la fédération à l'aide de la CloudTrail console ou de EnableFederationl'opération API. AWS CLI Lorsque vous activez la fédération de requêtes Lake, vous CloudTrail créez une base de données gérée nommée `aws:cloudtrail` (si la base de données n'existe pas déjà) et une table fédérée gérée dans le catalogue de AWS Glue données. L'ID du magasin de données d'événements est utilisé pour le nom de la table. CloudTrail enregistre le rôle de fédération dans lequel l'ARN et le stockage des données d'événements sont stockés AWS Lake Formation, le service chargé de permettre un contrôle d'accès précis aux ressources fédérées du catalogue de données. AWS Glue

Pour activer la fédération de requêtes Lake, vous devez créer un rôle IAM ou choisir un rôle existant. Lake Formation utilise ce rôle pour gérer les autorisations pour le magasin de données d'événement fédéré. Lorsque vous créez un nouveau rôle à l'aide de la CloudTrail console, les autorisations requises sont CloudTrail automatiquement créées pour le rôle. Si vous choisissez un rôle existant, assurez-vous qu'il fournit les autorisations minimales.

Vous pouvez désactiver la fédération à l'aide de la CloudTrail console ou de DisableFederationl'opération API. AWS CLI Lorsque vous désactivez la fédération, l'intégration avec AWS Glue AWS Lake Formation, et Amazon Athena est CloudTrail désactivée. Après avoir désactivé la fédération de requêtes Lake, vous ne pouvez plus interroger les données de vos événements dans Athena. Aucune donnée de CloudTrail Lake n'est supprimée lorsque vous désactivez la fédération et vous pouvez continuer à exécuter des requêtes dans CloudTrail Lake.

La fédération d' CloudTrail un magasin de données d'événements CloudTrail Lake est gratuite. L'exécution de requêtes dans Amazon Athena entraîne des frais. Pour en savoir plus sur la tarification, consultez la Tarification d'Amazon Athena.

Analysez les journaux d'activité avec AWS CloudTrail Lake et Amazon Athena

Rubriques

Considérations

Tenez compte des facteurs suivants lors de la fédération d'un magasin de données d'événement :

- La fédération d' CloudTrail un magasin de données d'événements CloudTrail Lake est gratuite. L'exécution de requêtes dans Amazon Athena entraîne des frais. Pour en savoir plus sur la tarification, consultez la Tarification d'Amazon Athena.
- Lake Formation est utilisée pour gérer les autorisations pour les ressources fédérées. Si vous supprimez le rôle de fédération, ou si vous révoquez les autorisations d'accès aux ressources de Lake Formation AWS Glue, vous ne pouvez pas exécuter de requêtes depuis Athena. Pour plus d'informations sur l'utilisation de Lake Formation, veuillez consulter la page Gérer les ressources de la fédération des CloudTrail lacs avec AWS Lake Formation.
- Toute personne utilisant Amazon Athena pour interroger des données enregistrées dans Lake Formation doit disposer d'une politique d'autorisations IAM qui autorise l'action `lakeformation:GetDataAccess`. La politique AWS gérée : AmazonAthenaFullAccessautorise cette action. Si vous utilisez des politiques en ligne, veillez à mettre à jour les politiques d'autorisations afin d'autoriser cette action. Pour plus d'informations, consultez la page Gestion des autorisations de Lake Formation et des utilisateurs d'Athena.
- Pour créer des vues sur des tables fédérées dans Athena, vous avez besoin d'une base de données de destination autre que `aws:cloudtrail`. Cela est dû au fait que la `aws:cloudtrail` base de données est gérée par CloudTrail.
- Pour créer un ensemble de données dans Amazon QuickSight, vous devez choisir l'option Utiliser un code SQL personnalisé. Pour plus d'informations, consultez Créer un jeu de données à l'aide des données Amazon Athena.

- Si la fédération est activée, vous ne pouvez pas supprimer un magasin de données d'événement. Pour supprimer un magasin de données d'événement fédéré, vous devez d'abord désactiver la fédération et la protection contre la résiliation si elle est activée.
- Les considérations suivantes s'appliquent aux magasins de données d'événement de l'organisation :
  - Un seul compte administrateur délégué ou le compte de gestion peut activer la fédération sur le magasin de données d'événement d'une organisation. Les autres comptes administrateur délégué peuvent toujours interroger et partager des informations à l'aide de la fonctionnalité de partage de données de Lake Formation.
  - Tout compte administrateur délégué ou le compte de gestion de l'organisation peut désactiver la fédération.

Autorisations nécessaires pour la fédération

Avant de fédérer un magasin de données d'événement, assurez-vous de disposer de toutes les autorisations requises pour le rôle de fédération et pour activer et désactiver la fédération. Vous devez uniquement mettre à jour les autorisations du rôle de fédération si vous choisissez un rôle IAM existant pour activer la fédération. Si vous choisissez de créer un nouveau rôle IAM à l'aide de la CloudTrail console, CloudTrail fournit toutes les autorisations nécessaires pour le rôle.

Rubriques

- Autorisations IAM pour fédérer un magasin de données d'événement
- Autorisations requises pour activer la fédération
- Autorisations nécessaires pour désactiver la fédération

Autorisations IAM pour fédérer un magasin de données d'événement

Lorsque vous activez la fédération, vous pouvez créer un nouveau rôle IAM ou utiliser un rôle IAM existant. Lorsque vous choisissez un nouveau rôle IAM, vous CloudTrail créez un rôle IAM avec les autorisations requises et aucune autre action n'est requise de votre part.

Si vous choisissez un rôle existant, assurez-vous que les politiques du rôle IAM fournissent les autorisations requises pour activer la fédération. Cette section fournit des exemples de politiques d'approbation et d'autorisation requises du rôle IAM.

L'exemple suivant fournit la politique d'autorisation pour le rôle de fédération. Pour la première instruction, fournissez l'ARN complet de votre magasin de données d'événement pour le paramètre `Resource`.

La deuxième instruction de cette politique permet à Lake Formation de déchiffrer les données d'un magasin de données d'événement chiffré à l'aide d'une clé KMS. Remplacez *`key-region`*, *`account-id`* et *`key-id`* par les valeurs de votre clé KMS. Vous pouvez omettre cette instruction si votre magasin de données d'événement n'utilise pas de clé KMS pour le chiffrement.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

L'exemple suivant fournit la politique d'approbation IAM, qui permet à AWS Lake Formation d'endosser un rôle IAM pour gérer les autorisations pour le magasin de données d'événement fédéré.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Autorisations requises pour activer la fédération

L'exemple de politique suivant fournit les autorisations minimales requises pour activer la fédération sur un magasin de données d'événement. Cette politique permet d' CloudTrail activer la fédération sur le magasin de données d'événements, AWS Glue de créer les ressources fédérées dans le catalogue de AWS Glue données et de AWS Lake Formation gérer l'enregistrement des ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
```

```
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Autorisations nécessaires pour désactiver la fédération

L'exemple de politique suivant fournit les ressources minimales requises pour désactiver la fédération dans un magasin de données d'événement. Cette politique permet de CloudTrail désactiver la fédération sur le magasin de données d'événements, de AWS Glue supprimer la table fédérée gérée dans le catalogue de AWS Glue données et de Lake Formation de désenregistrer la ressource fédérée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
```

```
        {
            "Sid": "Allow Lake Formation to deregister the resource",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Activer la fédération de requêtes Lake

Vous pouvez activer la fédération de requêtes Lake à l'aide de la CloudTrail AWS CLI console ou de EnableFederationl'API. Lorsque vous activez la fédération de requêtes Lake, vous CloudTrail créez une base de données gérée nommée `aws:cloudtrail` (si la base de données n'existe pas déjà) et une table fédérée gérée dans le catalogue de AWS Glue données. L'ID du magasin de données d'événements est utilisé pour le nom de la table. CloudTrail enregistre le rôle de fédération dans lequel l'ARN et le stockage des données d'événements sont stockés AWS Lake Formation, le service chargé de permettre un contrôle d'accès précis aux ressources fédérées du catalogue de données. AWS Glue

Cette section décrit comment activer la fédération à l'aide de la CloudTrail console et AWS CLI.

CloudTrail console

La procédure suivante explique comment activer la fédération de requêtes Lake sur un magasin de données d'événement existant.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Magasins de données d'événement.
3. Choisissez le magasin de données d'événement que vous voulez mettre à jour. Cela ouvre la page contenant les détails du magasin de données d'événement.
4. Dans Fédération de requêtes Lake, choisissez Modifier, puis sélectionnez Activer.
5. Choisissez de créer un nouveau rôle IAM ou d'utiliser un rôle IAM existant. Lorsque vous créez un nouveau rôle, il en crée CloudTrail automatiquement un avec les autorisations requises. Si vous utilisez un rôle existant, assurez-vous que la politique du rôle fournit les autorisations minimales requises.
6. Si vous créez un nouveau rôle IAM, saisissez un nom pour identifier le rôle.

7. Si vous choisissez un rôle IAM existant, choisissez le rôle que vous souhaitez utiliser. Le rôle doit exister dans votre compte.
8. Sélectionnez Enregistrer les modifications. Le statut de la fédération passe à `Enabled`.

AWS CLI

Pour activer la fédération, exécutez la commande aws cloudtrail enable-federation en fournissant les paramètres --event-data-store et --role requis. Pour --event-data-store, fournissez l'ARN du magasin de données d'événement (ou le suffixe d'ID de l'ARN). Pour --role, fournissez l'ARN correspondant à votre rôle de fédération. Le rôle doit exister dans votre compte et fournir les autorisations minimales requises.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Cet exemple montre comment un administrateur délégué peut activer la fédération sur le magasin de données d'événement d'organisation en spécifiant l'ARN du magasin de données d'événement dans le compte de gestion et l'ARN du rôle de fédération dans le compte administrateur délégué.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Désactiver la fédération de requêtes Lake

Vous pouvez désactiver la fédération à l'aide de la CloudTrail console ou de DisableFederationl'opération API. AWS CLI Lorsque vous désactivez la fédération, l'intégration avec AWS Glue AWS Lake Formation, et Amazon Athena est CloudTrail désactivée. Après avoir désactivé la fédération de requêtes Lake, vous ne pouvez plus interroger les données de vos événements dans Athena. Aucune donnée de CloudTrail Lake n'est supprimée lorsque vous désactivez la fédération et vous pouvez continuer à exécuter des requêtes dans CloudTrail Lake.

Cette section décrit comment désactiver la fédération à l'aide de la CloudTrail console et AWS CLI.

CloudTrail console

La procédure suivante explique comment désactiver la fédération de requêtes Lake sur un magasin de données d'événement existant.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Magasins de données d'événement.
3. Choisissez le magasin de données d'événement que vous voulez mettre à jour. Cela ouvre la page contenant les détails du magasin de données d'événement.
4. Dans Fédération de requêtes Lake, choisissez Modifier, puis Désactiver.
5. Sélectionnez Enregistrer les modifications. Le statut de la fédération passe à `Disabled`.

AWS CLI

Pour désactiver la fédération sur le magasin de données d'événement, exécutez la commande aws cloudtrail disable-federation. Le magasin de données d'événement est spécifié par `--event-data-store`, qui accepte un ARN de magasin de données d'événement ou le suffixe d'ID de l'ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> S'il s'agit du magasin de données d'événement d'organisation, vous devez utiliser l'ID du compte de gestion.

Gérer les ressources de la fédération des CloudTrail lacs avec AWS Lake Formation

Lorsque vous fédérez un magasin de données d'événements, CloudTrail enregistrez le rôle de fédération ARN et le magasin de données d'événements AWS Lake Formation, le service chargé de permettre un contrôle d'accès précis aux ressources fédérées du catalogue de données. AWS Glue Cette section décrit comment vous pouvez utiliser Lake Formation pour gérer les ressources de la fédération des CloudTrail lacs.

Lorsque vous activez la fédération, CloudTrail crée les ressources suivantes dans le catalogue de AWS Glue données.

- Base de données gérée : CloudTrail crée une base de données avec le nom `aws:cloudtrail` de chaque compte. CloudTrail gère la base de données. Vous ne pouvez ni supprimer ni modifier la base de données dans AWS Glue.
- Table fédérée gérée : CloudTrail crée une table pour chaque banque de données d'événements fédérée et utilise l'ID de la banque de données d'événements pour le nom de la table. CloudTrail gère les tables. Vous ne pouvez ni supprimer ni modifier les tables dans AWS Glue. Pour supprimer une table, vous devez désactiver la fédération dans le magasin de données d'événement.

Contrôle de l'accès aux ressources fédérées

Vous pouvez utiliser l'une des deux méthodes d'autorisation pour contrôler l'accès à la base de données et aux tables gérées.

- Contrôle d'accès IAM uniquement : avec le contrôle d'accès IAM uniquement, tous les utilisateurs du compte disposant des autorisations IAM requises ont accès à toutes les ressources du catalogue de données. Pour plus d'informations sur le AWS Glue fonctionnement avec IAM, voir AWS Glue Fonctionnement avec IAM.

  Sur la console Lake Formation, cette méthode apparaît sous la forme Utiliser uniquement le contrôle d'accès IAM.

  > **Note**
  >
  > Si vous souhaitez créer des filtres de données et utiliser d'autres fonctionnalités de Lake Formation, vous devez utiliser le contrôle d'accès de Lake Formation.

- Contrôle d'accès à Lake Formation : cette méthode offre les avantages suivants.
  - Vous pouvez implémenter la sécurité au niveau des colonnes, des lignes et des cellules en créant des filtres de données.
  - La base de données et les tables ne sont visibles que par les administrateurs de Lake Formation et les créateurs de la base de données et des ressources. Si un autre utilisateur a besoin d'accéder à ces ressources, vous devez explicitement accorder l'accès en utilisant les autorisations de Lake Formation.

Pour plus d'informations sur le contrôle d'accès, consultez la page Méthodes de contrôle d'accès précis.

Déterminer la méthode d'autorisation pour une ressource fédérée

Lorsque vous activez la fédération pour la première fois, CloudTrail crée une base de données gérée et une table fédérée gérée en utilisant les paramètres de votre lac de données de Lake Formation.

Après avoir CloudTrail activé la fédération, vous pouvez vérifier la méthode d'autorisation que vous utilisez pour la base de données gérée et la table fédérée gérée en vérifiant les autorisations pour ces ressources. Si le paramètre `ALL` (Super) défini sur `IAM_ALLOWED_PRINCIPALS` est présent pour la ressource, celle-ci est gérée exclusivement par des autorisations IAM. Si le paramètre est absent, la ressource est gérée par les autorisations de Lake Formation. Pour plus d'informations sur les autorisations Lake Formation, consultez la page Référence des autorisations Lake Formation.

La méthode d'autorisation pour la base de données gérée et la table fédérée gérée peuvent être différentes. Par exemple, si vous vérifiez les valeurs de la base de données et de la table, vous pouvez voir ce qui suit :

- Pour la base de données, la valeur qui attribue `ALL` (Super) à `IAM_ALLOWED_PRINCIPALS` est présente dans les autorisations, ce qui indique que vous utilisez uniquement le contrôle d'accès IAM pour la base de données.
- Pour la table, la valeur qui attribue `ALL` (Super) à `IAM_ALLOWED_PRINCIPALS` n'est pas présente, ce qui indique un contrôle d'accès par les permissions de Lake Formation.

Vous pouvez passer d'une méthode d'accès à l'autre à tout moment en ajoutant ou en supprimant l'autorisation `ALL` (Super) définie sur `IAM_ALLOWED_PRINCIPALS` sur n'importe quelle ressource fédérée de Lake Formation.

Partage entre comptes à l'aide de Lake Formation

Cette section décrit comment partager une base de données gérée et une table fédérée gérée entre des comptes à l'aide de Lake Formation.

Vous pouvez partager une base de données gérée entre plusieurs comptes en procédant comme suit :

1. Mettez à jour la version de partage de données entre comptes vers la version 4.
2. Supprimez les autorisations `Super` définies sur `IAM_ALLOWED_PRINCIPALS` de la base de données si elles sont présentes pour passer au contrôle d'accès à Lake Formation.

3. Accordez des autorisations `Describe` au compte externe sur la base de données.
4. Si une ressource du catalogue de données est partagée avec vous Compte AWS et que votre compte n'appartient pas à la même AWS organisation que le compte de partage, acceptez l'invitation de partage de ressources provenant de AWS Resource Access Manager (AWS RAM). Pour plus d'informations, voir Accepter une invitation de partage de ressources depuis la AWS RAM.

Une fois ces étapes terminées, la base de données devrait être visible par le compte externe. Par défaut, le partage de la base de données ne donne accès à aucune table de la base de données.

Vous pouvez partager toutes les tables fédérées gérées ou certaines d'entre elles avec un compte externe en procédant comme suit :

1. Mettez à jour la version de partage de données entre comptes vers la version 4.
2. Supprimez les autorisations `Super` définies sur `IAM_ALLOWED_PRINCIPALS` de la table si elles sont présentes pour passer au contrôle d'accès à Lake Formation.
3. (Facultatif) Spécifiez les filtres de données pour restreindre les colonnes ou les lignes.
4. Accordez des autorisations `Select` au compte externe sur la table.
5. Si une ressource du catalogue de données est partagée avec vous Compte AWS et que votre compte n'appartient pas à la même AWS organisation que le compte de partage, acceptez l'invitation de partage de ressources provenant de AWS Resource Access Manager (AWS RAM). Pour une organisation, vous pouvez l'accepter automatiquement à l'aide des paramètres RAM. Pour plus d'informations, voir Accepter une invitation de partage de ressources depuis la AWS RAM.
6. La table devrait maintenant être visible. Pour activer les requêtes Amazon Athena sur cette table, créez un lien de ressource dans ce compte avec la table partagée.

Le compte propriétaire peut révoquer le partage à tout moment en supprimant les autorisations pour le compte externe de Lake Formation ou en désactivant la fédération dans. CloudTrail

Magasins de données d'événement d'organisation

Si vous avez créé une organisation dans AWS Organizations, vous pouvez créer un magasin de données d'événements d'organisation qui enregistre tous les événements pour tous Comptes AWS les membres de cette organisation. Les banques de données sur les événements de l'organisation peuvent s'appliquer à toutes les Régions AWS organisations ou à la région actuelle. Les magasins

de données d'événement d'organisation ne peuvent pas être utilisés pour collecter des événements externes à AWS.

Vous pouvez créer un magasin de données d'événements d'organisation à l'aide du compte de gestion ou du compte d'administrateur délégué. Lorsqu'un administrateur délégué crée un magasin de données d'événement d'organisation, celui-ci existe dans le compte de gestion de l'organisation. Cette approche s'explique par le fait que le compte de gestion conserve la propriété de toutes les ressources de l'organisation.

Le compte de gestion d'une organisation peut mettre à jour un magasin de données d'événements au niveau du compte pour l'appliquer à une organisation.

Lorsque le magasin de données d'événement d'organisation est spécifié comme s'appliquant à une organisation, il est automatiquement appliqué à tous les comptes membres de l'organisation. Les comptes membres ne peuvent pas afficher le magasin de données d'événement d'organisation, ni le modifier ou le supprimer. Par défaut, les comptes membres n'ont pas accès au magasin de données d'événement d'organisation et ne peuvent pas exécuter de requêtes sur ce type de magasins.

Le tableau suivant présente les fonctionnalités du compte de gestion et des comptes d'administrateur délégué au sein de l' AWS Organizations organisation.

Fonctionnalités	Compte de gestion	Compte administrateur délégué
Enregistrer ou supprimer les comptes administrateur délégué.	Oui	Non
Créez un magasin de données d'événements d'organisation pour les AWS CloudTrail événements ou les éléments AWS Config de configuration.	Oui	Oui
Activer Insights sur le magasin de données d'événement d'organisation.	Oui	Non
Mettre à jour un magasin de données d'événement d'organisation.	Oui	Oui[1]

Fonctionnalités	Compte de gestion	Compte administrateur délégué
Activer la fédération de requêtes Lake sur le magasin de données d'événement d'organisation.[2]	Oui	Oui
Désactiver la fédération de requêtes Lake dans un magasin de données d'événement d'organisation.	Oui	Oui
Supprimer un magasin de données d'événement d'organisation.	Oui	Oui
Copier des événements de journal de suivi dans un magasin de données d'événement.	Oui	Non
Exécuter des requêtes sur des magasins de données d'événement d'organisation.	Oui	Oui
Consultez le tableau de bord CloudTrail Lake pour le magasin de données sur les événements d'une organisation.	Oui	Oui

[1] Seul le compte de gestion peut convertir un magasin de données d'événements d'organisation en un magasin de données d'événements au niveau du compte, ou convertir un magasin de données d'événements au niveau du compte en un magasin de données d'événements d'organisation. Ces actions ne sont pas autorisées pour l'administrateur délégué, car les magasins de données d'événement d'organisation n'existent que dans le compte de gestion. Lorsque le magasin de données d'événements d'une organisation est converti en un magasin de données d'événements au niveau du compte, seul le compte de gestion a accès au magasin de données d'événements. De même, seul un magasin de données d'événements au niveau du compte dans le compte de gestion peut être converti en magasin de données d'événements d'organisation.

[2]Un seul compte administrateur délégué ou le compte de gestion peut activer la fédération dans le magasin de données d'événement d'organisation. D'autres comptes administrateur délégué peuvent interroger et partager des informations à l'aide de la fonctionnalité de partage de données de Lake

Formation. Tout compte administrateur délégué ainsi que le compte de gestion de l'organisation peuvent désactiver la fédération.

Création d'une banque de données sur les événements d'une organisation

Le compte de gestion ou le compte d'administrateur délégué d'une organisation peut créer un magasin de données d'événements d'organisation pour collecter des CloudTrail événements (événements de gestion, événements de données) ou des éléments AWS Config de configuration.

> **Note**
>
> Seul le compte de gestion de l'organisation peut copier les événements du parcours dans un magasin de données d'événements.

CloudTrail console

Pour créer un magasin de données d'événements d'organisation à l'aide de la console

1. Suivez les étapes de la procédure de création d'un magasin de données d' CloudTrail événements pour créer un magasin de données d'événements d'organisation pour CloudTrail la gestion ou les événements de données.

   OU

   Suivez les étapes de la procédure de création d'un magasin de données d'événements pour les éléments de AWS Config configuration afin de créer un magasin de données d'événements d'organisation pour les éléments AWS Config de configuration.
2. Sur la page Choisir des événements, choisissez Activer pour tous les comptes de mon organisation.

AWS CLI

Pour créer un magasin de données d'événements d'organisation, exécutez la create-event-data-storecommande et incluez l'`--organization-enabled`option.

L'exemple de AWS CLI `create-event-data-store` commande suivant crée un magasin de données d'événements d'organisation qui collecte tous les événements de gestion. Étant donné que CloudTrail les événements de gestion sont enregistrés par défaut, il n'est pas nécessaire

de spécifier des sélecteurs d'événements avancés si votre banque de données d'événements enregistre tous les événements de gestion et ne collecte aucun événement de données.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

L'exemple de AWS CLI `create-event-data-store` commande suivant crée un magasin de données d'événements d'organisation nommé `config-items-org-eds` qui collecte les éléments AWS Config de configuration. Pour collecter des éléments de configuration, spécifiez que le `eventCategory` champ est égal `ConfigurationItem` dans les sélecteurs d'événements avancés.

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
```

```
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Appliquer un magasin de données d'événements au niveau du compte à une organisation

Le compte de gestion de l'organisation peut convertir un magasin de données d'événements au niveau du compte pour l'appliquer à une organisation.

CloudTrail console

Pour mettre à jour un magasin de données d'événements au niveau du compte à l'aide de la console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Magasins de données d'événement.
3. Choisissez le magasin de données d'événement que vous voulez mettre à jour. Cette action ouvre la page contenant les détails du magasin de données d'événement.
4. Dans General details (Détails généraux), choisissez Edit (Modifier).
5. Choisissez Activer pour tous les comptes de mon organisation.
6. Sélectionnez Enregistrer les modifications.

Pour plus d'informations sur la mise à jour d'une banque de données d'événements, consultezMettre à jour un magasin de données d'événements avec la console.

AWS CLI

Pour mettre à jour un magasin de données d'événements au niveau du compte afin de l'appliquer à une organisation, exécutez la update-event-data-storecommande et incluez l'`--organization-enabled`option.

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Consultez aussi

- Administrateur délégué de l'organisation
- Ajouter un administrateur CloudTrail délégué
- Supprimer un administrateur CloudTrail délégué

Créez une intégration avec une source d'événements en dehors de AWS

Vous pouvez l'utiliser CloudTrail pour enregistrer et stocker les données d'activité des utilisateurs provenant de n'importe quelle source dans vos environnements hybrides, comme les applications internes ou SaaS hébergées sur site ou dans le cloud, les machines virtuelles ou les conteneurs. Vous pouvez stocker ces données, y accéder, effectuer des analyses, résoudre des problèmes et agir sur celles-ci sans avoir à gérer plusieurs agrégateurs de journaux et outils de création de rapports.

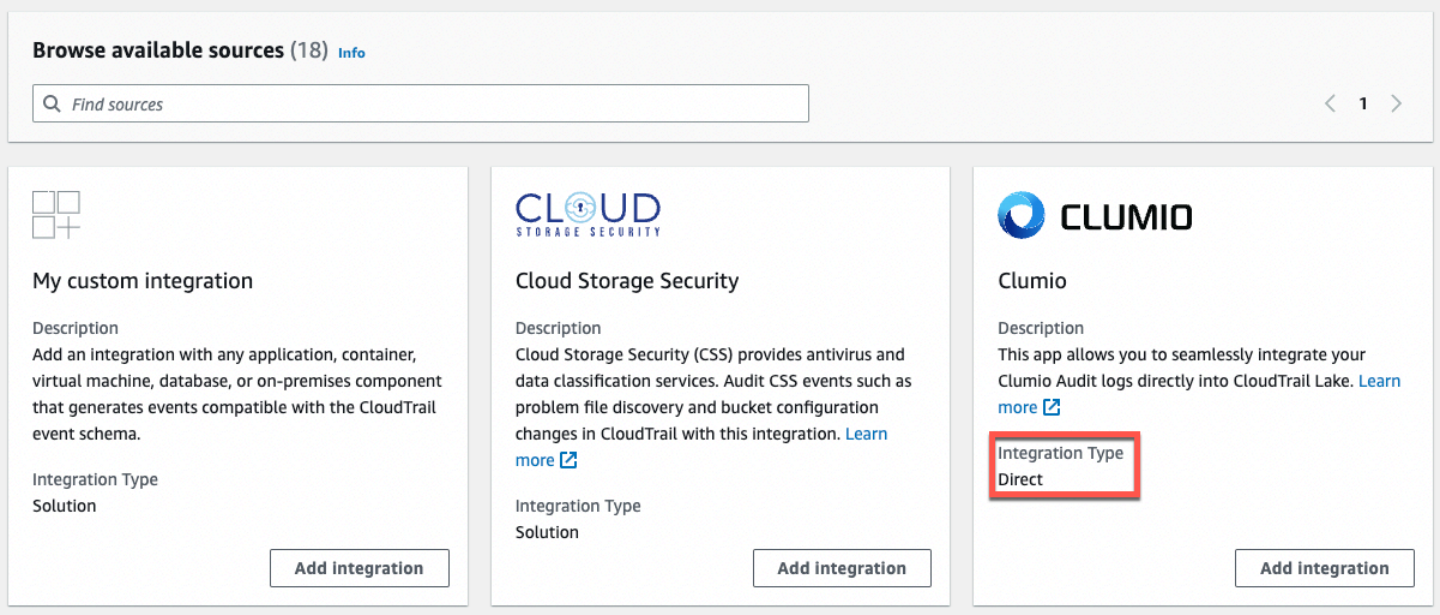
Les événements d'activités AWS provenant de sources externes utilisent des canaux pour diffuser dans CloudTrail Lake des événements provenant de partenaires externes qui travaillent avec CloudTrail vous ou provenant de vos propres sources. Lorsque vous créez un canal, vous sélectionnez un ou plusieurs magasins de données d'événement pour stocker les événements provenant de la source du canal. Vous pouvez modifier les stockages de données d'événement de destination d'un canal selon vos besoins, à condition qu'ils soient configurés pour journaliser les événements `eventCategory="ActivityAuditLog"`. Lorsque vous créez un canal pour les événements d'un partenaire externe, vous fournissez un ARN de canal au partenaire ou à l'application source. La politique de ressources attachée au canal permet à la source de transmettre des événements via celui-ci. Si un canal ne dispose d'aucune politique de ressources, seul le propriétaire du canal peut appeler l'API `PutAuditEvents` sur celui-ci.

CloudTrail a établi un partenariat avec de nombreux fournisseurs de sources d'événements, tels qu'Okta et LaunchDarkly. Lorsque vous créez une intégration avec une source d'événements externe AWS, vous pouvez choisir l'un de ces partenaires comme source d'événements, ou choisir

Mon intégration personnalisée pour y intégrer des événements provenant de vos propres sources CloudTrail. Un seul canal est autorisé par source.

Il existe deux types d'intégrations : directe et solution. Dans le cas des intégrations directes, le partenaire appelle l'`PutAuditEvents`API pour transmettre les événements au magasin de données d'événements de votre AWS compte. Avec les intégrations de solutions, l'application s'exécute dans votre AWS compte et l'application appelle l'`PutAuditEvents`API pour transmettre les événements au magasin de données d'événements de votre AWS compte.

Sur la page Integrations (Intégrations), vous pouvez sélectionner l'onglet Available sources (Sources disponibles) afin d'afficher Integration type (Type d'intégration) pour les partenaires.



Pour commencer, créez une intégration pour consigner les événements provenant de partenaires ou d'autres sources d'applications à l'aide de la CloudTrail console.

Rubriques

- Créez une intégration avec un CloudTrail partenaire à l'aide de la console
- Création d'une intégration personnalisée avec la console
- Créez, mettez à jour et gérez les intégrations de CloudTrail Lake avec le AWS CLI
- Informations supplémentaires sur les partenaires d'intégration
- CloudTrail Schéma des événements Lake Integrations

Créez une intégration avec un CloudTrail partenaire à l'aide de la console

Lorsque vous créez une intégration avec une source d'événements extérieure AWS, vous pouvez choisir l'un de ces partenaires comme source d'événements. Lorsque vous créez une intégration dans CloudTrail une application partenaire, le partenaire a besoin du nom de ressource Amazon (ARN) du canal que vous créez dans ce flux de travail pour envoyer des événements CloudTrail. Après avoir créé l'intégration, vous terminez de configurer l'intégration en suivant les instructions du partenaire pour lui fournir l'ARN de canal requis. L'intégration commence à intégrer les événements des partenaires une CloudTrail fois que le partenaire a appelé `PutAuditEvents` le canal de l'intégration.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Intégrations.
3. Sur la page Ajouter une intégration, saisissez un nom pour votre chaîne. Le nom doit comporter entre 3 et 128 caractères. Les noms peuvent contenir uniquement des lettres, des chiffres, des points, des tirets et des traits de soulignement.
4. Sélectionnez la source d'application partenaire à partir de laquelle vous souhaitez obtenir des événements. Si vous intégrez des événements à partir de vos propres applications hébergées sur site ou dans le cloud, sélectionnez My custom integration (Mon intégration personnalisée).
5. Dans Emplacement de réception des événements, choisissez de journaliser ces événements d'activité dans des magasins de données d'événement existants ou d'en créer un nouveau.

   Si vous choisissez de créer un nouveau magasin de données d'événement, saisissez un nom pour celui-ci et spécifiez la période de conservation en jours. Le magasin de données d'événement conserve les données d'événement pendant le nombre de jours spécifié.

   Si vous choisissez de journaliser les événements d'activité dans un ou plusieurs magasins de données d'événement existants, sélectionnez-les dans la liste. Les stockages de données d'événement ne peuvent inclure que des événements d'activité. Le type d'événement dans la console doit être Events from integrations (Événements issus des intégrations). Dans l'API, la valeur `eventCategory` doit être `ActivityAuditLog`.
6. Dans Resource policy (Politique de ressources), configurez la politique de ressources pour le canal de l'intégration. Les politiques de ressources sont des documents de politique JSON précisant les actions qu'un principal spécifié peut effectuer sur la ressource ainsi que les conditions dans lesquelles ces actions peuvent être effectuées. Les comptes définis comme principaux dans la politique de ressources peuvent appeler l'API `PutAuditEvents`

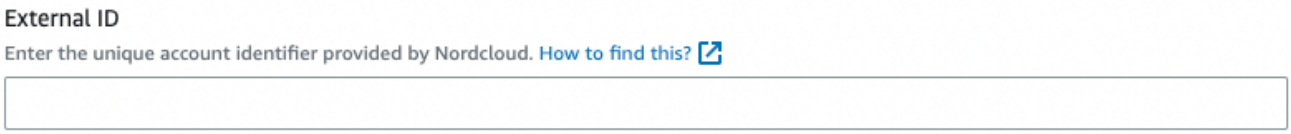
pour transmettre des événements à votre canal. Le propriétaire de la ressource dispose d'un accès implicite à la ressource si sa politique IAM autorise l'action `cloudtrail-data:PutAuditEvents`.

Les informations requises pour la politique sont déterminées par le type d'intégration. Pour une intégration des directions, ajoute CloudTrail automatiquement les identifiants de AWS compte du partenaire et vous demande de saisir l'identifiant externe unique fourni par le partenaire. Pour une intégration de solution, vous devez spécifier au moins un identifiant de AWS compte comme identifiant principal, et vous pouvez éventuellement saisir un identifiant externe pour éviter toute confusion entre les adjoints.

> **Note**
>
> Si vous ne créez pas de politique de ressources pour le canal, seul son propriétaire peut appeler l'API `PutAuditEvents` sur celui-ci.

a. Pour une intégration directe, saisissez l'ID externe fourni par votre partenaire. Le partenaire d'intégration fournit un ID externe unique, tel qu'un ID de compte ou une chaîne générée aléatoirement, à utiliser pour l'intégration afin d'éviter tout problème d'adjoint confus. Le partenaire est responsable de la création et de la transmission d'un ID externe unique.

   Vous pouvez sélectionner How to find this? (Comment trouver cela ?) pour consulter la documentation du partenaire expliquant comment trouver l'ID externe.

   > **Note**
   >
   > Si la politique de ressources inclut un ID externe, tous les appels à l'API `PutAuditEvents` doivent l'inclure. Cependant, si la politique ne définit pas d'ID externe, le partenaire peut appeler l'API `PutAuditEvents` et spécifier un paramètre `externalId`.

b. Pour une intégration de solution, choisissez Ajouter un AWS compte pour spécifier un ID de AWS compte à ajouter en tant que principal dans la politique.

7. (Facultatif) Dans la zone Tags (Balises), vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre stockage de données d'événement. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises dans AWS, consultez la section AWS Ressources de balisage dans le Références générales AWS.
8. Lorsque vous souhaitez créer la nouvelle intégration, sélectionnez Ajouter une intégration. Il n'y a pas de page d'évaluation. CloudTrail crée l'intégration, mais vous devez fournir le nom de ressource Amazon (ARN) du canal à l'application partenaire. Les instructions pour fournir l'ARN du canal à l'application partenaire se trouvent sur le site Web de documentation du partenaire. Afin d'obtenir davantage d'informations et ouvrir la page du partenaire dans AWS Marketplace, cliquez sur le lien Learn more (En savoir plus) pour le partenaire dans l'onglet Available sources (Sources disponibles) de la page Integrations (Intégrations).

Afin de terminer la configuration de votre intégration, fournissez l'ARN du canal au partenaire ou à l'application source. Selon le type d'intégration, vous, le partenaire ou l'application exécutez l'API `PutAuditEvents` pour transmettre les événements d'activité au stockage de données d'événement de votre compte AWS . Une fois vos événements d'activité transmis, vous pouvez utiliser CloudTrail Lake pour rechercher, interroger et analyser les données enregistrées par vos applications. Les données de votre événement incluent des champs correspondant à la charge utile de l' CloudTrailévénement, tels que `eventVersion`, `eventSource`, et`userIdentity`.

Création d'une intégration personnalisée avec la console

Vous pouvez l'utiliser CloudTrail pour enregistrer et stocker les données d'activité des utilisateurs provenant de n'importe quelle source dans vos environnements hybrides, comme les applications internes ou SaaS hébergées sur site ou dans le cloud, les machines virtuelles ou les conteneurs. Effectuez la première moitié de cette procédure dans la console CloudTrail Lake, puis appelez l'`PutAuditEvents`API pour ingérer les événements, en fournissant l'ARN de votre canal et la charge utile des événements. Après avoir utilisé l'`PutAuditEvents`API pour intégrer l'activité de votre application CloudTrail, vous pouvez utiliser CloudTrail Lake pour rechercher, interroger et analyser les données enregistrées par vos applications.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Intégrations.

3. Sur la page Ajouter une intégration, saisissez un nom pour votre chaîne. Le nom doit comporter entre 3 et 128 caractères. Les noms peuvent contenir uniquement des lettres, des chiffres, des points, des tirets et des traits de soulignement.
4. Sélectionnez My custom integration (Mon intégration personnalisée).
5. Dans Event delivery location (Emplacement de réception des événements), choisissez de journaliser ces événements d'activité dans des stockages de données d'événement existants ou d'en créer un nouveau.

   Si vous choisissez de créer un nouveau magasin de données d'événement, saisissez un nom pour celui-ci et spécifiez la période de conservation en jours. Vous pouvez conserver les données d'événement dans une banque de données d'événement jusqu'à 3 653 jours (environ 10 ans) si vous choisissez l'option de tarification de rétention extensible d'un an, ou jusqu'à 2 557 jours (environ 7 ans) si vous choisissez l'option de tarification de rétention de sept ans.

   Si vous choisissez de journaliser les événements d'activité dans un ou plusieurs magasins de données d'événement existants, sélectionnez-les dans la liste. Les stockages de données d'événement ne peuvent inclure que des événements d'activité. Le type d'événement dans la console doit être Events from integrations (Événements issus des intégrations). Dans l'API, la valeur `eventCategory` doit être `ActivityAuditLog`.
6. Dans Resource policy (Politique de ressources), configurez la politique de ressources pour le canal de l'intégration. Les politiques de ressources sont des documents de politique JSON précisant les actions qu'un principal spécifié peut effectuer sur la ressource ainsi que les conditions dans lesquelles ces actions peuvent être effectuées. Les comptes définis comme principaux dans la politique de ressources peuvent appeler l'API `PutAuditEvents` pour transmettre des événements à votre canal.

   > **Note**
   >
   > Si vous ne créez pas de politique de ressources pour le canal, seul son propriétaire peut appeler l'API `PutAuditEvents` sur celui-ci.

   a. (Facultatif) Entrez un ID externe unique pour fournir un niveau de protection supplémentaire. L'ID externe est une chaîne unique, telle qu'un ID de compte ou une chaîne générée aléatoirement, pour éviter tout problème d'adjoint confus.

> **Note**
>
> Si la politique de ressources inclut un ID externe, tous les appels à l'API `PutAuditEvents` doivent l'inclure. Cependant, si la politique ne définit aucun ID externe, vous pouvez appeler l'API `PutAuditEvents` et spécifier un paramètre `externalId`.

b. Choisissez Ajouter un AWS compte pour spécifier chaque identifiant de AWS compte à ajouter en tant que principal dans la politique de ressources de la chaîne.

7. (Facultatif) Dans la zone Tags (Balises), vous pouvez ajouter jusqu'à 50 paires clé-valeur de balise pour vous aider à identifier, trier et contrôler l'accès à votre stockage de données d'événement. Pour plus d'informations sur l'utilisation des politiques IAM pour autoriser l'accès à un magasin de données d'événement basé sur des identifications, consultez Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications. Pour plus d'informations sur la manière dont vous pouvez utiliser les balises dans AWS, voir Marquer vos AWS ressources dans le Références générales AWS.
8. Lorsque vous souhaitez créer la nouvelle intégration, sélectionnez Ajouter une intégration. Il n'y a pas de page d'évaluation. CloudTrail crée l'intégration, mais pour intégrer vos événements personnalisés, vous devez spécifier l'ARN du canal dans une `PutAuditEvents`demande.
9. Appelez l'`PutAuditEvents`API pour y intégrer CloudTrail les événements de votre activité. Vous pouvez ajouter jusqu'à 100 événements d'activité (ou jusqu'à 1 Mo) par demande `PutAuditEvents`. Vous aurez besoin de l'ARN du canal que vous avez créé au cours des étapes précédentes, de la charge utile des événements que vous CloudTrail souhaitez ajouter et de l'ID externe (si spécifié dans votre politique de ressources). Assurez-vous que la charge utile de l'événement ne contient aucune information sensible ou d'identification personnelle avant de l'ingérer. CloudTrail Les événements auxquels vous participez CloudTrail doivent suivre leCloudTrail Schéma des événements Lake Integrations.

> **Tip**
>
> AWS CloudShellUtilisez-le pour vous assurer que vous utilisez les AWS API les plus récentes.

Les exemples suivants montrent comment utiliser la commande de la CLI put-audit-events. Les paramètres --audit-events et --channel-arn sont obligatoires. Vous avez besoin de l'ARN

du canal que vous avez créé lors des étapes précédentes. Vous pouvez le copier depuis la page des détails de l'intégration. La valeur de --audit-events est un tableau JSON d'objets d'événements. `--audit-events`inclut un identifiant requis pour l'événement, la charge utile requise de l'événement comme valeur de`EventData`, et une somme de contrôle facultative pour aider à valider l'intégrité de l'événement après son ingestion. CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

Voici un exemple de commande avec deux exemples d'événement.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

L'exemple de commande suivant ajoute le paramètre `--cli-input-json` pour spécifier un fichier JSON (`custom-events.json`) de charge utile d'événement.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

Voici les exemples de contenu de l'exemple de fichier JSON, `custom-events.json`.

```
{
    "auditEvents": [
      {
```

```
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

(Facultatif) Calcul d'une valeur de somme de contrôle

La somme de contrôle que vous spécifiez comme valeur de `EventDataChecksum` dans une `PutAuditEvents` demande vous permet de vérifier qui CloudTrail reçoit l'événement correspondant à la somme de contrôle ; elle permet de vérifier l'intégrité des événements. La valeur de la somme de contrôle est un algorithme base64-SHA256 que vous calculez en exécutant la commande suivante.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
       \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
       \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
       \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
       \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
       \"additionalEventData\":{\"key\":\"value\"},
       \"sourceIPAddress\":\"source_IP_address\",
       \"recipientAccountId\":\"recipient_account_ID\"}",
       "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

La commande renvoie la somme de contrôle. Voici un exemple.

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

La valeur de la somme de contrôle devient la valeur de `EventDataChecksum` dans votre demande `PutAuditEvents`. Si la somme de contrôle ne correspond pas à celle de l'événement fourni, CloudTrail rejette l'événement avec une `InvalidChecksum` erreur.

Créez, mettez à jour et gérez les intégrations de CloudTrail Lake avec le AWS CLI

Vous pouvez utiliser le AWS CLI pour créer, mettre à jour et gérer vos intégrations CloudTrail Lake. Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la Région AWS configuration adaptée à votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

Commandes disponibles pour les intégrations de CloudTrail Lake

Les commandes permettant de créer, de mettre à jour et de gérer les intégrations dans CloudTrail Lake incluent :

- `create-event-data-store`pour créer un magasin de données d'événements pour les événements extérieurs à AWS.
- `delete-channel`pour supprimer un canal utilisé pour une intégration.
- `delete-resource-policy`pour supprimer la politique de ressources attachée à un canal pour une intégration CloudTrail Lake.
- `get-channel`pour renvoyer des informations sur une CloudTrail chaîne.
- `get-resource-policy`pour récupérer le texte JSON du document de politique basé sur les ressources joint au CloudTrail canal.
- `list-channels`pour répertorier les chaînes du compte courant et leurs noms de source.
- `put-audit-events`pour ingérer les événements de votre application dans CloudTrail Lake. Paramètre obligatoire`auditEvents`, qui accepte les enregistrements JSON (également appelés charge utile) des événements que vous souhaitez CloudTrail ingérer. Vous pouvez ajouter jusqu'à 100 de ces événements (ou jusqu'à 1 Mo) par `PutAuditEvents` demande.
- `put-resource-policy`pour associer une politique d'autorisation basée sur les ressources à un CloudTrail canal utilisé pour une intégration avec une source d'événements extérieure à. AWS Pour plus d'informations sur les politiques basées sur les ressources, consultez les exemples de politiques basées sur les AWS CloudTrail ressources.
- `update-channel`pour mettre à jour un canal spécifié par un ARN ou un UUID de canal requis.

Pour obtenir la liste des commandes disponibles pour les magasins de données d'événements CloudTrail Lake, consultezCommandes disponibles pour les magasins de données d'événements.

Pour obtenir la liste des commandes disponibles pour les requêtes CloudTrail Lake, consultezCommandes disponibles pour les requêtes CloudTrail Lake.

Créez une intégration pour enregistrer les événements extérieurs à l' AWS aide du AWS CLI

Dans le AWS CLI, vous créez une intégration qui enregistre les événements extérieurs AWS à l'aide de quatre commandes (trois si vous disposez déjà d'un magasin de données d'événements répondant aux critères). Les magasins de données d'événements que vous utilisez comme destinations pour une intégration doivent être destinés à une seule région et à un seul compte ; ils ne peuvent pas être multirégionaux, ils ne peuvent pas enregistrer les événements des organisations dans AWS Organizations lesquelles ils se trouvent et ils ne peuvent inclure que des événements d'activité. Le type d'événement dans la console doit être Events from integrations (Événements issus des intégrations). Dans l'API, la valeur `eventCategory` doit être `ActivityAuditLog`. Pour plus d'informations sur les intégrations, veuillez consulter la section Créez une intégration avec une source d'événements en dehors de AWS.

1. Si vous ne disposez d'aucun stockage de données d'événement que vous pouvez utiliser pour l'intégration, exécutez create-event-data-store pour en créer un.

   L'exemple de AWS CLI commande suivant crée un magasin de données d'événements qui enregistre les événements extérieurs AWS. Pour les événements d'activité, la valeur du sélecteur de champ `eventCategory` est `ActivityAuditLog`. Le stockage de données d'événement a une période de conservation de 90 jours. Par défaut, le magasin de données d'événements collecte les événements de toutes les régions, mais comme il ne collecte pas d'AWS événements, définissez-le sur une seule région en ajoutant l'`--no-multi-region-enabled`option. La protection contre la résiliation est activée par défaut et le stockage de données d'événement ne collecte pas d'événements pour les comptes d'une organisation.

   ```
   aws cloudtrail create-event-data-store \
   --name my-event-data-store \
   --no-multi-region-enabled \
   --retention-period 90 \
   --advanced-event-selectors '[
       {
         "Name": "Select all external events",
   ```

```
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Vous aurez besoin de l'ID du stockage de données d'événement (le suffixe de l'ARN, ou `EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE` dans l'exemple de réponse précédent) pour passer à l'étape suivante et créer votre canal.

2. Exécutez la create-channelcommande pour créer un canal permettant à un partenaire ou à une application source d'envoyer des événements vers un magasin de données d'événements dans CloudTrail.

Un canal dispose des composants suivants :

Source

CloudTrail utilise ces informations pour identifier les partenaires auxquels les données relatives aux événements sont envoyées CloudTrail en votre nom. Une source est requise et peut être `Custom` pour tous les événements externes àAWS valides, ou le nom d'une source d'événements partenaires. Un seul canal est autorisé par source.

Pour plus d'informations sur les valeurs `Source` des partenaires disponibles, veuillez consulter la section Informations supplémentaires sur les partenaires d'intégration.

Statut d'ingestion

Le statut du canal indique le moment auquel les derniers événements ont été reçus d'une source de canal.

Destinations

Les destinations sont les magasins de données d'événements du CloudTrail lac qui reçoivent les événements du canal. Vous pouvez modifier les stockages de données d'événement de destination pour un canal.

Pour ne plus recevoir d'événements provenant d'une source, supprimez le canal.

Afin d'exécuter cette commande, vous avez besoin d'au moins un ID de stockage de données d'événement de destination. Le type de destination valide est `EVENT_DATA_STORE`. Vous pouvez envoyer des événements ingérés vers plusieurs stockages de données d'événement. L'exemple de commande suivant crée un canal qui envoie des événements à deux stockages de données d'événement représentés par leurs ID dans l'attribut `Location` du paramètre `--destinations`. Les paramètres `--destinations`, `--name` et `--source` sont obligatoires. Pour ingérer les événements d'un CloudTrail partenaire, spécifiez le nom du partenaire comme valeur de`--source`. Pour ingérer des événements provenant de vos propres applications externes AWS, spécifiez `Custom` comme valeur de`--source`.

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
```

```
    --name my-partner-channel \
    --source $partnerSourceName \
```

Dans la réponse à votre commande create-channel, copiez l'ARN du nouveau canal. Vous avez besoin de l'ARN pour exécuter les commandes `put-resource-policy` et `put-audit-events` au cours des étapes suivantes.

3. Exécutez la put-resource-policycommande pour associer une politique de ressources au canal. Les politiques de ressources sont des documents de politique JSON précisant les actions qu'un principal spécifié peut effectuer sur la ressource ainsi que les conditions dans lesquelles ces actions peuvent être effectuées. Les comptes définis comme principaux dans la politique de ressources du canal peuvent appeler l'API `PutAuditEvents` pour transmettre des événements.

> **Note**
>
> Si vous ne créez pas de politique de ressources pour le canal, seul son propriétaire peut appeler l'API `PutAuditEvents` sur celui-ci.

Les informations requises pour la politique sont déterminées par le type d'intégration.

- Pour une intégration directe, la politique CloudTrail doit contenir les identifiants de AWS compte du partenaire et vous oblige à saisir l'identifiant externe unique fourni par le partenaire. CloudTrail ajoute automatiquement les identifiants de AWS compte du partenaire à la politique de ressources lorsque vous créez une intégration à l'aide de la CloudTrail console. Reportez-vous à la documentation du partenaire pour savoir comment obtenir les numéros de AWS compte requis pour la police.
- Pour une intégration de solution, vous devez spécifier au moins un identifiant de AWS compte comme identifiant principal, et vous pouvez éventuellement saisir un identifiant externe pour éviter toute confusion entre les adjoints.

Voici les conditions requises pour la politique de ressources :

- L'ARN de ressource défini dans la politique doit correspondre à l'ARN du canal auquel la politique est attachée.
- La politique ne contient qu'une seule action : cloudtrail-data : PutAuditEvents
- La politique contient au moins une instruction. La politique peut comporter un maximum de 20 instructions.

- Chaque instruction comprend au moins un principal. Une instruction peut comporter un maximum de 50 principaux.

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

Pour plus d'informations sur les stratégies de ressources, consultez AWS CloudTrail exemples de politiques basées sur les ressources.

4. Exécutez l'`PutAuditEvents`API pour y intégrer CloudTrail les événements de votre activité. Vous aurez besoin de la charge utile des événements que vous souhaitez CloudTrail ajouter.

Assurez-vous qu'aucune information sensible ou d'identification personnelle ne se trouve dans la charge utile de l'événement avant de l'ingérer. CloudTrail Notez que l'API `PutAuditEvents` utilise le point de terminaison CLI `cloudtrail-data`, et non le point de terminaison `cloudtrail`.

Les exemples suivants montrent comment utiliser la commande de la CLI put-audit-events. Les paramètres --audit-events et --channel-arn sont obligatoires. Le paramètre --external-id est requis si un ID externe est défini dans la politique de ressources. Vous avez besoin de l'ARN du canal que vous avez créé à l'étape précédente. La valeur de --audit-events est un tableau JSON d'objets d'événements. `--audit-events`inclut un identifiant requis pour l'événement, la charge utile requise de l'événement comme valeur de`EventData`, et une somme de contrôle facultative pour aider à valider l'intégrité de l'événement après son ingestion. CloudTrail

```
aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

Voici un exemple de commande avec deux exemples d'événement.

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

L'exemple de commande suivant ajoute le paramètre `--cli-input-json` pour spécifier un fichier JSON (`custom-events.json`) de charge utile d'événement.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

Voici les exemples de contenu de l'exemple de fichier JSON, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

Vous pouvez vérifier que l'intégration fonctionne et CloudTrail qu'elle intègre correctement les événements provenant de la source en exécutant la get-channelcommande. La sortie de get-channel indique l'horodatage le plus récent ayant CloudTrail reçu des événements.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(Facultatif) Calcul d'une valeur de somme de contrôle

La somme de contrôle que vous spécifiez comme valeur de `EventDataChecksum` dans une `PutAuditEvents` demande vous permet de vérifier qui CloudTrail reçoit l'événement correspondant à la somme de contrôle ; elle permet de vérifier l'intégrité des événements. La valeur de la somme de contrôle est un algorithme base64-SHA256 que vous calculez en exécutant la commande suivante.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
       \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
       \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
       \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
       \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
       \"additionalEventData\":{\"key\":\"value\"},
       \"sourceIPAddress\":\"source_IP_address\",
       \"recipientAccountId\":\"recipient_account_ID\"}",
       "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

La commande renvoie la somme de contrôle. Voici un exemple.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

La valeur de la somme de contrôle devient la valeur de `EventDataChecksum` dans votre demande `PutAuditEvents`. Si la somme de contrôle ne correspond pas à celle de l'événement fourni, CloudTrail rejette l'événement avec une `InvalidChecksum` erreur.

Mettez à jour une chaîne avec le AWS CLI

Exécutez la commande update-channel pour mettre à jour le nom d'un canal ou les magasins de données d'événement de destination. Le paramètre `--channel` est obligatoire. Vous ne pouvez pas mettre à jour la source d'un canal. Voici un exemple.

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

Supprimer une chaîne pour supprimer une intégration avec AWS CLI

Pour arrêter d'ingérer des événements liés à un partenaire ou à d'autres activités extérieures AWS, supprimez le canal en exécutant la delete-channel commande. L'ARN ou l'ID de canal (le suffixe ARN) du canal que vous souhaitez supprimer est obligatoire. Voici un exemple.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

Informations supplémentaires sur les partenaires d'intégration

Le tableau de cette section fournit le nom source de chaque partenaire d'intégration et identifie le type d'intégration (directe ou solution).

Les informations de la colonne Source name (Nom de source) sont requises lors de l'appel de l'API `CreateChannel`. Vous spécifiez le nom de la source comme valeur pour le paramètre `Source`.

Nom du partenaire (console)	Nom de la source (API)	Type d'intégration
Mon intégration personnalisée	`Custom`	solution
Sécurité du stockage dans le cloud	`CloudStorageSecurityConsole`	solution
Clumio	`Clumio`	directe
CrowdStrike	`CrowdStrike`	solution
CyberArk	`CyberArk`	solution
GitHub	`GitHub`	solution
Kong Inc	`KongGatewayEnterprise`	solution
LaunchDarkly	`LaunchDarkly`	directe
Netskope	`NetskopeCloudExchange`	solution
Nordcloud, une société d'IBM	`IBMMulticloud`	directe
MontyCloud	`MontyCloud`	directe
Okta	`OktaSystemLogEvents`	solution

Nom du partenaire (console)	Nom de la source (API)	Type d'intégration
One Identity	`OneLogin`	solution
Shoreline.io	`Shoreline`	solution
Snyk.io	`Snyk`	directe
Wiz	`WizAuditLogs`	solution

Consulter la documentation des partenaires

Vous pouvez en savoir plus sur l'intégration d'un partenaire à CloudTrail Lake en consultant sa documentation.

Pour consulter la documentation des partenaires

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Intégrations.
3. Sur la page Intégrations, sélectionnez Sources disponibles, puis En savoir plus pour le partenaire dont vous souhaitez consulter la documentation.

CloudTrail Schéma des événements Lake Integrations

Le tableau suivant décrit les éléments de schéma obligatoires et facultatifs qui correspondent à ceux des enregistrements CloudTrail d'événements. Le contenu de `eventData` est fourni par vos événements ; les autres champs sont fournis par CloudTrail After ingestion.

CloudTrail le contenu des enregistrements d'événements est décrit plus en détail dansCloudTrail enregistrer le contenu.

- Champs fournis par CloudTrail After ingestion
- Champs fournis par vos événements

Champs fournis par CloudTrail After ingestion

Nom de champ	Type d'entrée	Exigence	Description
eventVersion	chaîne	Obligatoire	La version de l'événement.
eventCategory	chaîne	Obligatoire	Catégorie de l'événement. Pour les AWS événements non liés, la valeur est `ActivityAuditLog` .
eventType	chaîne	Obligatoire	Type d'événement. Pour les AWS événements non liés, la valeur valide est `ActivityLog` .
eventID	chaîne	Obligatoire	ID unique pour un événement.
eventTime	chaîne	Obligatoire	Horodatage de l'événement, au format `yyyy-MM-DDTHH:mm:ss` , en temps universel coordonné (UTC).
awsRegion	chaîne	Obligatoire	L' Région AWS endroit où l'`PutAuditEvents` appel a été passé.
recipientAccountId	chaîne	Obligatoire	Représente l'ID du compte qui a reçu cet événement. CloudTrai

Nom de champ	Type d'entrée	Exigence	Description
			l remplit ce champ en le calculant à partir de la charge utile de l'événement.
addendum	-	Facultatif	Affiche des informations sur la raison pour laquelle le traitement des événements a été retardé. Si des informations manquaient dans un événement existant, le bloc d'addendum inclut les informations manquantes et la raison de leur absence.
• raison	chaîne	Facultatif	La raison pour laquelle l'événement ou une partie de son contenu est manquant.
• updatedFields	chaîne	Facultatif	Les champs d'enregistrement d'événement qui sont mis à jour par l'addenda. Ceci n'est fourni que si la raison est `UPDATED_DATA` .

Nom de champ	Type d'entrée	Exigence	Description
• originalUID	chaîne	Facultatif	L'UID d'événement d'origine provenant de la source. Ceci n'est fourni que si la raison est `UPDATED_DATA` .
• originalEventID	chaîne	Facultatif	L'ID d'événement d'origine. Ceci n'est fourni que si la raison est `UPDATED_DATA` .
métadonnées	-	Obligatoire	Informations sur le canal utilisé par l'événement.
• ingestionTime	chaîne	Obligatoire	L'horodatage du traitement de l'événement, au format `yyyy-MM-DDTHH:mm:ss` , en temps universel coordonné (UTC).
• channelARN	chaîne	Obligatoire	L'ARN du canal utilisé par l'événement.

Champs fournis par les événements client

Nom de champ	Type d'entrée	Exigence	Description
eventData	-	Obligatoire	Les données d'audit envoyées CloudTrail lors d'un `PutAuditEvents` appel.

Nom de champ	Type d’entrée	Exigence	Description
• version	chaîne	Obligatoire	La version de l'événement de sa source. Contraintes de longueur : longueur maximale de 256.
• userIdentity	-	Obligatoire	Informations sur l'utilisateur qui a émis une demande.
• • type	chaîne	Obligatoire	Le type d'identité de l'utilisateur. Contraintes de longueur : longueur maximale de 128.
• • principalId	chaîne	Obligatoire	Un identifiant unique pour l'acteur de l'événement. Contraintes de longueur : longueur maximale de 1 024.
• • détails	Objet JSON	Facultatif	Informations supplémentaires sur l'identité.

Nom de champ	Type d'entrée	Exigence	Description
• userAgent	chaîne	Facultatif	Agent par le biais duquel la demande a été effectuée. Contraintes de longueur : longueur maximale de 1 024.
• eventSource	chaîne	Obligatoire	Il s'agit de la source d'événements partenaires ou de l'application personnalisée de laquelle les événements sont journalisés. Contraintes de longueur : longueur maximale de 1 024.
• eventName	chaîne	Obligatoire	L'action demandée, l'une des actions de l'API pour le service ou l'application source. Contraintes de longueur : longueur maximale de 1 024.
• eventTime	chaîne	Obligatoire	Horodatage de l'événement, au format `yyyy-MM-DDTHH:mm:ss` , en temps universel coordonné (UTC).

Nom de champ	Type d'entrée	Exigence	Description
• UID	chaîne	Obligatoire	La valeur UID qui identifie la demande. Le service ou l'applica tion appelé(e) génère cette valeur. Contraintes de longueur : longueur maximale de 1 024.
• requestParameters	Objet JSON	Facultatif	Les paramètres, le cas échéant, qui ont été envoyées avec la demande. Ce champ a une taille maximale de 100 Ko, tout contenu dépassant cette limite est rejeté.
• responseElements	Objet JSON	Facultatif	L'élément de réponse pour les actions qui apportent des modifications (actions de création, mise à jour ou suppressi ons). Ce champ a une taille maximale de 100 Ko, tout contenu dépassant cette limite est rejeté.

Nom de champ	Type d'entrée	Exigence	Description
• errorCode	chaîne	Facultatif	Une chaîne représentant une erreur pour l'événement. Contraintes de longueur : longueur maximale de 256.
• errorMessage	chaîne	Facultatif	La description de l'erreur. Contraintes de longueur : longueur maximale de 256.
• sourceIPAddress	chaîne	Facultatif	Adresse IP à partir de laquelle la demande a été effectuée. Les adresses IPv4 et IPv6 sont acceptées.
• recipientAccountId	chaîne	Obligatoire	Représente l'ID du compte qui a reçu cet événement. L'identifiant du compte doit être le même que celui du AWS compte propriétaire de la chaîne.

Nom de champ	Type d'entrée	Exigence	Description
• additionalEventData	Objet JSON	Facultatif	Des données supplémentaires sur l'événement qui ne faisaient pas partie de la demande ou de la réponse. Ce champ a une taille maximale de 28 Ko, tout contenu dépassant cette limite est rejeté.

L'exemple suivant montre la hiérarchie des éléments de schéma qui correspondent à ceux des enregistrements CloudTrail d'événements.

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
       "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
```

```
            JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

Afficher les tableaux de bord de CloudTrail Lake

Vous pouvez utiliser les tableaux de bord CloudTrail Lake pour visualiser les événements dans un magasin de données d'événements. Vous pouvez choisir parmi plusieurs types de tableaux de bord. Les types de tableaux de bord disponibles pour un entrepôt de données d'événement dépendent de la configuration des sélecteurs d'événements avancés de l'entrepôt de données d'événement. Par exemple, si un type de tableau de bord affiche des informations sur les événements de CloudTrail gestion, vous ne pouvez sélectionner le tableau de bord que si le magasin de données d'événements actuellement sélectionné collecte CloudTrail des événements de gestion.

Chaque type de tableau de bord est composé de plusieurs widgets et chaque widget représente une requête SQL. Pour afficher la requête d'un widget, choisissez Afficher et analyser dans l'éditeur de requêtes pour ouvrir l'éditeur de requêtes. Vous ne pouvez pas modifier la requête générée par le système qui est utilisée pour remplir le widget, mais vous pouvez apporter des modifications à la requête et l'exécuter dans l'éditeur de requêtes pour une analyse plus approfondie.

Pour remplir et mettre à jour un tableau de bord, choisissez Exécuter des requêtes. Lorsque vous choisissez Exécuter les requêtes, CloudTrail exécute les requêtes générées par le système en votre nom. Étant donné que l'exécution des requêtes entraîne des coûts, vous CloudTrail demande de confirmer les coûts associés à l'exécution des requêtes. Il s'agit d'une confirmation unique. Pour plus d'informations sur la CloudTrail tarification, consultez la section CloudTrail Tarification.

Rubriques

Limites

Les limitations suivantes s'appliquent à la version actuelle.

- La version actuelle ne prend pas en charge les tableaux de bord, les widgets ou les requêtes personnalisés.
- La version actuelle fournit uniquement des tableaux de bord pour les magasins de données d'événements qui collectent des CloudTrail événements (événements de données, événements de gestion) et des événements Insights.
- La version actuelle ne prend pas en charge la modification des requêtes générées par le système utilisées pour remplir le tableau de bord. Vous pouvez afficher et modifier la requête sous-jacente pour n'importe quel widget dans l'onglet Éditeur de requêtes. Toutefois, toute modification apportée à la requête est destinée à une analyse supplémentaire en dehors du tableau de bord.

Prérequis

Les conditions préalables suivantes s'appliquent aux tableaux de bord Lake.

- Pour afficher et utiliser les tableaux de bord de Lake, vous devez créer au moins un magasin de données d'événements CloudTrail Lake. Vous pouvez créer des magasins de données d'événements à l'aide de la console ou de kits SDK. AWS CLI Pour plus d'informations sur la création d'un entrepôt de données d'événement à l'aide de la console, veuillez consulter Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

Pour plus d'informations sur la création d'un magasin de données d'événements à l'aide du AWS CLI, voirCréez, mettez à jour et gérez des banques de données d'événements à l'aide du AWS CLI.

- Pour remplir le tableau de bord, CloudTrail exécute des requêtes en votre nom. La première fois que vous consultez la page Tableaux de bord, il vous CloudTrail est demandé de confirmer les coûts associés à l'exécution des requêtes. Choisissez J'accepte de prendre en charge les frais d'exécution des requêtes.

Choisir un tableau de bord

Utilisez la procédure suivante pour choisir un entrepôt de données d'événement et un type de tableau de bord à afficher.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation de gauche, sous Lake, choisissez Tableau de bord.
3. Sélectionnez l'entrepôt de données d'événement pour lequel vous souhaitez visualiser des données.
4. Choisissez le type de tableau de bord que vous souhaitez afficher. La liste des tableaux de bord est remplie en fonction de la configuration des sélecteurs d'événements avancés de l'entrepôt de données d'événement sélectionné.

   Les types de tableaux de bord possibles sont les suivants.

   - Tableau de bord d'ensemble : affiche les utilisateurs les plus actifs Régions AWS, et Services AWS par nombre d'événements. Vous pouvez également consulter des informations sur l'activité des événements de gestion `read` et `write`, les événements les plus limités et les principales erreurs. Ce tableau de bord est disponible pour les entrepôts de données d'événement qui collectent des événements de gestion.
   - Tableau de bord Événements de gestion : affiche les événements de connexion à la console, les événements de refus d'accès, les actions destructrices et les principales erreurs par utilisateur. Vous pouvez également consulter des informations sur les versions TLS et les appels TLS périmés par utilisateur. Ce tableau de bord est disponible pour les entrepôts de données d'événement qui collectent des événements de gestion.
   - Tableau de bord Événements de données S3 : affiche l'activité du compte S3, les objets S3 les plus consultés, les principaux utilisateurs S3 et les principales actions S3. Ce tableau de bord

est disponible pour les entrepôts de données d'événement qui collectent des événements de données Amazon S3.

- Tableau de bord Événements Insights : affiche la proportion globale d'événements Insights par type Insights, la proportion d'événements Insights par type Insights pour les principaux utilisateurs et services, et le nombre d'événements Insights par jour. Le tableau de bord inclut également un widget qui répertorie jusqu'à 30 jours d'événements Insights. Ce tableau de bord n'est disponible que pour les entrepôts de données d'événement qui collectent des événements Insights.

> **Note**
>
> - Une fois que vous avez activé CloudTrail Insights pour la première fois dans le magasin de données d'événements source, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée. Pour plus d'informations, consultez Comprendre la diffusion d'événements Insights.
> - Le tableau de bord Événements Insights n'affiche que les informations relatives aux événements Insights collectés par l'entrepôt de données d'événement sélectionné, qui sont déterminées par la configuration de l'entrepôt de données d'événement source. Par exemple, si vous configurez l'entrepôt de données d'événement source pour activer les événements Insights sur `ApiCallRateInsight`, mais pas sur `ApiErrorRateInsight`, vous ne verrez aucune information sur les événements Insights sur `ApiErrorRateInsight`.

5. Choisissez de filtrer les données du tableau de bord par Plage absolue ou Plage relative. Choisissez Plage absolue pour sélectionner une plage de dates et d'heures spécifique. Choisissez Plage relative pour sélectionner une plage de temps prédéfinie ou une plage personnalisée. Par défaut, le tableau de bord affiche les données des événements des dernières 24 heures.

> **Note**
>
> CloudTrail Les requêtes Lake entraînent des coûts en fonction de la quantité de données numérisées. Pour aider à contrôler les coûts, vous pouvez filtrer sur une plage de temps plus restreinte. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

6. Choisissez Exécuter les requêtes pour exécuter les requêtes pour les widgets du tableau de bord.

Filtrer un tableau de bord sur une plage de dates ou d'heures

Par défaut, le tableau de bord affiche les données des dernières 24 heures. Vous pouvez filtrer un tableau de bord en fonction d'une Plage absolue ou d'une Plage relative.

Choisissez Plage absolue pour sélectionner une plage de dates et d'heures spécifique.

Choisissez Plage relative pour sélectionner une plage de temps prédéfinie ou une plage personnalisée.

Après avoir choisi la plage horaire, choisissez Exécuter les requêtes pour actualiser le tableau de bord.

> **Note**
>
> CloudTrail Les requêtes Lake entraînent des coûts en fonction de la quantité de données numérisées. Pour aider à contrôler les coûts, vous pouvez filtrer sur une plage de temps plus restreinte. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Afficher la requête pour un widget de tableau de bord

Chaque widget représente une requête SQL. Pour afficher la requête d'un widget, choisissez Afficher et analyser dans l'éditeur de requêtes pour ouvrir l'éditeur de requêtes. À l'aide de l'éditeur de requêtes, vous pouvez affiner la requête en dehors du tableau de bord et exécuter la requête pour voir les résultats de votre requête mise à jour. Pour plus d'informations sur l'utilisation des requêtes, veuillez consulter Créer ou modifier une requête.

> **Note**
>
> Vous ne pouvez pas modifier la requête générée par le système pour un widget de tableau de bord. Toutes les modifications apportées à la requête dans l'onglet Éditeur de requêtes sont uniquement destinées à une analyse plus approfondie en dehors du tableau de bord.

CloudTrail Requêtes sur le lac

Les requêtes dans CloudTrail Lake sont créées en SQL. Vous pouvez créer une requête dans l'onglet CloudTrail Lake Editor en écrivant la requête en SQL à partir de zéro, ou en ouvrant une requête enregistrée ou un exemple de requête et en la modifiant. Vous ne pouvez pas remplacer un exemple de requête inclus par vos modifications, mais vous pouvez l'enregistrer en tant que nouvelle requête. Pour plus d'informations sur le langage de requête SQL autorisé, consultez CloudTrail Contraintes SQL du lac.

Une requête sans limite (telle que `SELECT * FROM edsID`) analyse toutes les données de votre magasin de données d'événement. Pour aider à contrôler les coûts, nous vous recommandons de limiter les requêtes en ajoutant des horodatages `eventTime` de début et de fin aux requêtes. L'exemple suivant montre comment rechercher tous les événements dans un magasin de données d'événement spécifié où l'heure de l'événement est postérieure au (>) 5 janvier 2023 à 13 h 51 et antérieure au (<) 19 janvier 2023 à 13 h 51. Étant donné qu'un magasin de données d'événement comporte une période de conservation minimale de sept jours, la durée minimale entre les valeurs de début et de fin `eventTime` est également de sept jours.

```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

Rubriques

- Outils d'éditeur de requête
- Afficher des exemples de requêtes dans la CloudTrail console
- Créer ou modifier une requête
- Exécuter une requête et enregistrer les résultats
- Afficher les résultats des requêtes
- Téléchargement des résultats enregistrés d'une requête
- Validation des résultats enregistrés d'une requête
- Exécutez et gérez les requêtes CloudTrail Lake à l'aide du AWS CLI

Outils d'éditeur de requête

Une barre d'outils située en haut à droite de l'éditeur de requêtes propose des commandes permettant de créer et de formater votre requête SQL.

Les sections suivantes décrivent les commandes de la barre d'outils.

- Undo (Annuler) : rétablit la dernière modification de contenu effectuée dans l'éditeur de requêtes.
- Redo (Rétablir) : répète la dernière modification de contenu effectuée dans l'éditeur de requêtes.
- Format sélectionné : organise le contenu de l'éditeur de requêtes selon les conventions de mise en forme et d'espacement SQL.
- Commenter/décommenter la sélection : commente la partie sélectionnée de la requête si elle n'est pas déjà commentée. Si la partie sélectionnée est déjà commentée, le choix de cette option supprime le commentaire.

Afficher des exemples de requêtes dans la CloudTrail console

La CloudTrail console fournit un certain nombre d'exemples de requêtes qui peuvent vous aider à commencer à écrire vos propres requêtes.

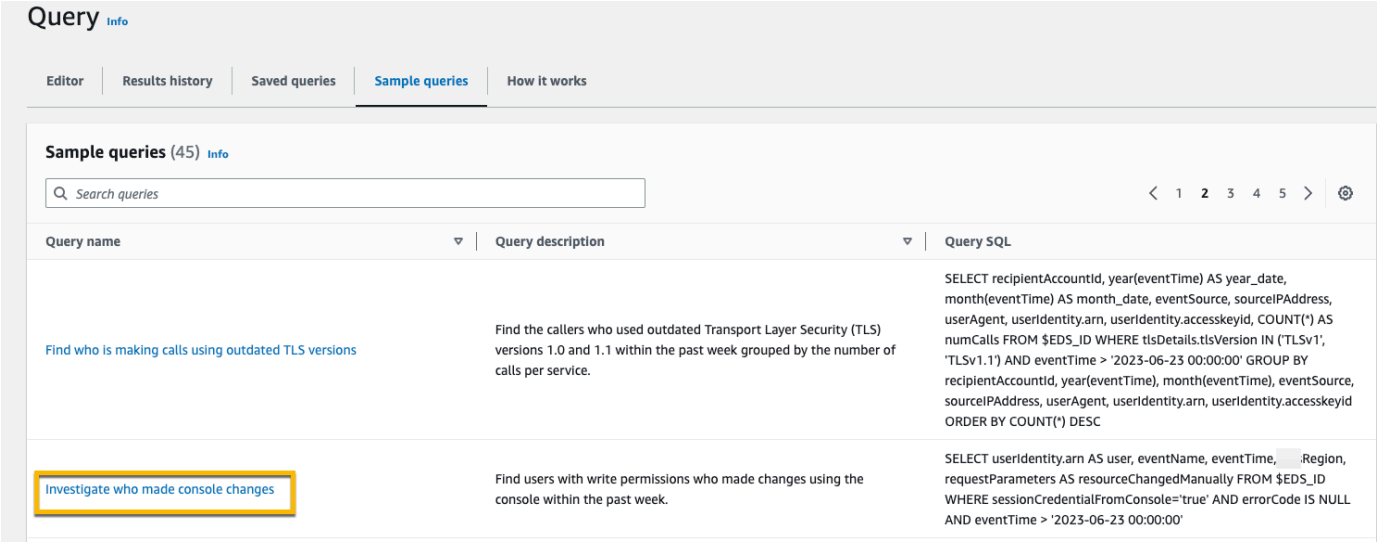
CloudTrail les requêtes sont facturées en fonction de la quantité de données numérisées. Pour aider à contrôler les coûts, nous vous recommandons de limiter les requêtes en ajoutant des horodatages `eventTime` de début et de fin aux requêtes. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

> **Note**
>
> Vous pouvez également consulter les requêtes créées par la GitHub communauté. Pour plus d'informations et pour consulter ces exemples de requêtes, voir CloudTrailLake sample queries sur le GitHub site Web. AWS CloudTrail n'a pas évalué les requêtes dans GitHub.

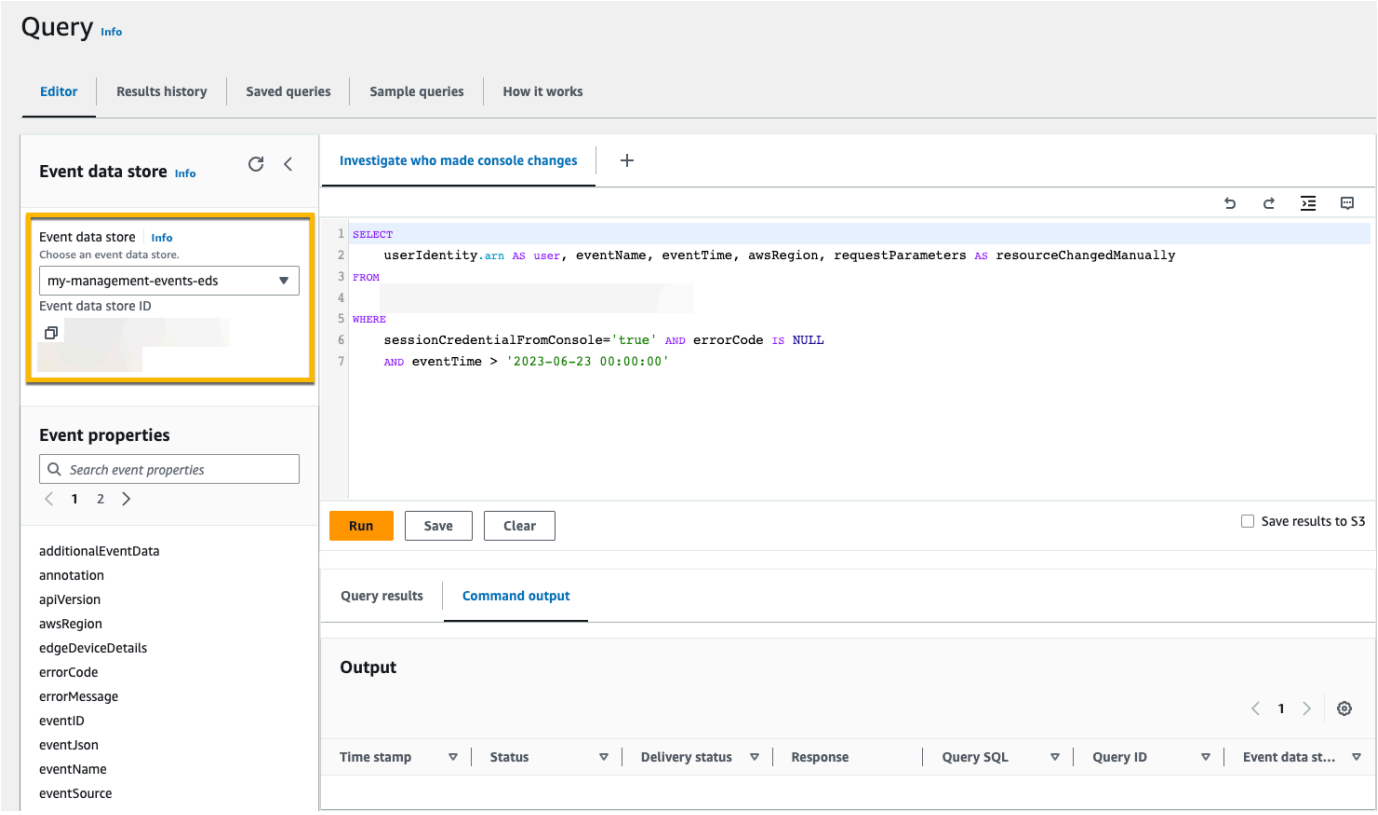
Pour afficher et exécuter un exemple de requête

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.

2. Dans le panneau de navigation, sous Lake, choisissez Requête.
3. Sur la page Requête, sélectionnez l'onglet Exemples de requêtes.
4. Choisissez un exemple de requête dans la liste ou recherchez la requête pour filtrer la liste. Dans cet exemple, nous allons ouvrir la requête Investigate who made console changes en choisissant le Nom de la requête. Cela ouvre la requête dans l'onglet Éditeur.

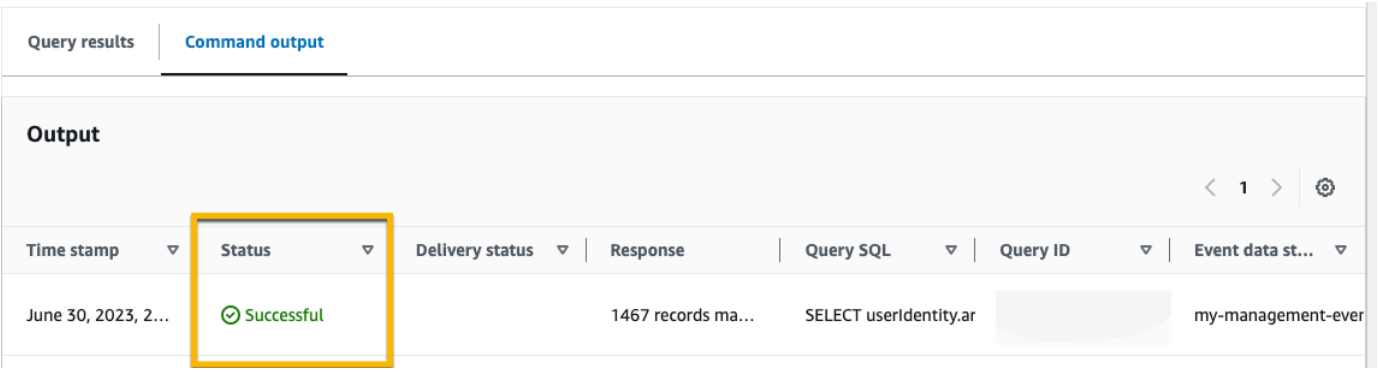


5. Dans l'onglet Éditeur, choisissez l'entrepôt de données d'événement pour lequel vous souhaitez exécuter la requête. Lorsque vous choisissez le magasin de données d'événements dans la liste, l'ID du magasin de données d'événements est CloudTrail automatiquement renseigné dans la `FROM` ligne de l'éditeur de requêtes.

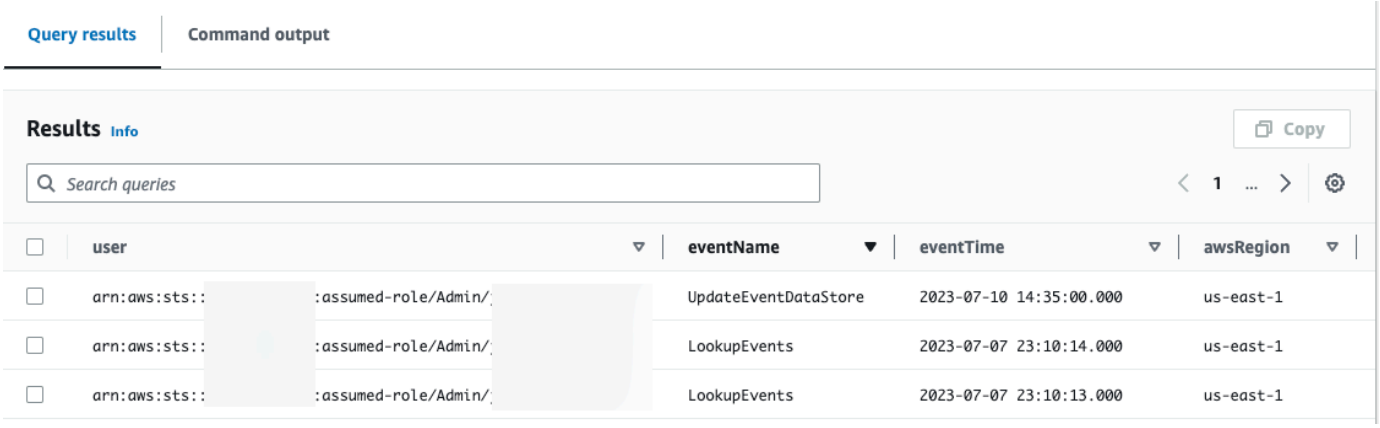


6. Choisissez Exécuter pour exécuter la requête.

   L'onglet Sortie de commande affiche les métadonnées relatives à votre requête, telles que le succès de la requête, le nombre d'enregistrements correspondants et la durée d'exécution de la requête.



   L'onglet Résultats de la requête affiche les données d'événements de l'entrepôt de données d'événement sélectionné qui correspondent à votre requête.



Pour plus d'informations sur l'édition d'une requête, veuillez consulter Créer ou modifier une requête. Pour plus d'informations sur l'exécution d'une requête et l'enregistrement des résultats, veuillez consulter Exécuter une requête et enregistrer les résultats.

Créer ou modifier une requête

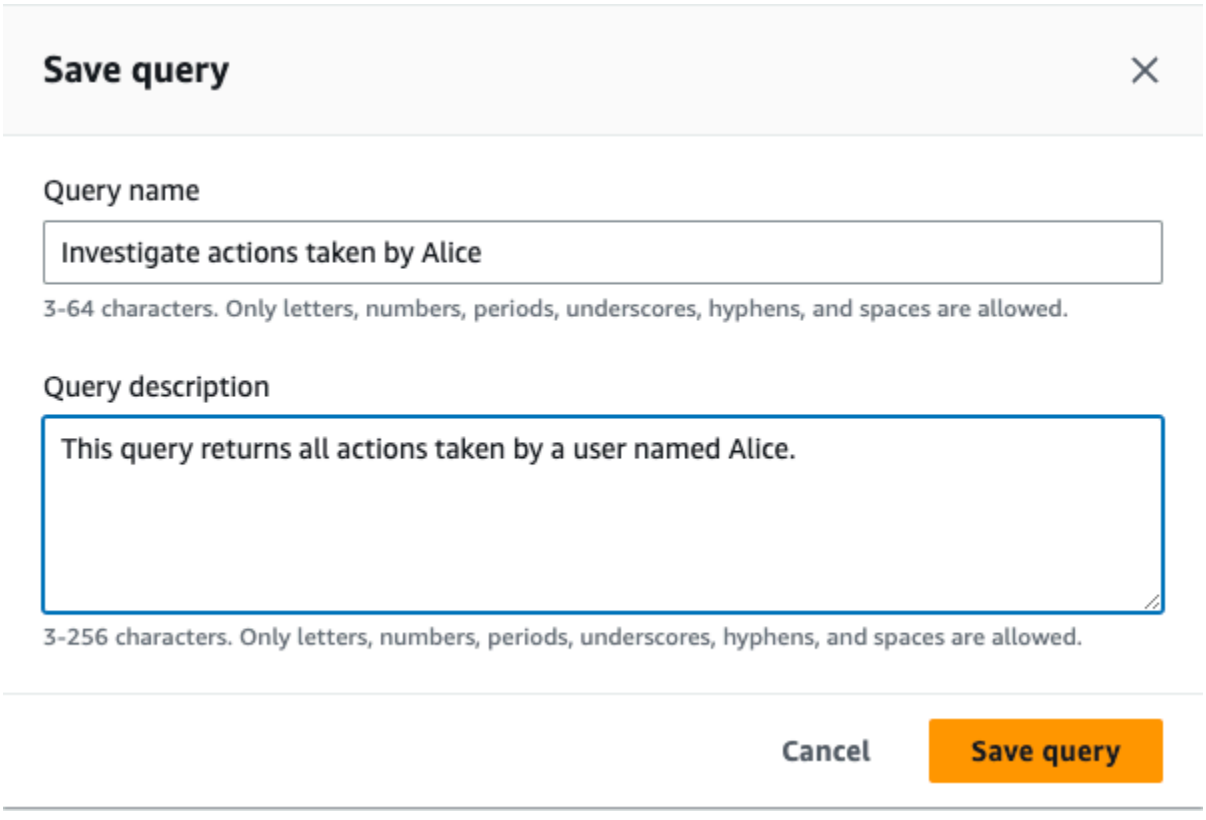
Dans cette procédure guidée, nous ouvrons l'un des exemples de requêtes, puis nous le modifions pour trouver les actions entreprises par un utilisateur spécifique nommé `Alice`, et nous l'enregistrons comme une nouvelle requête. Vous pouvez également modifier une requête enregistrée sur l'onglet Requêtes enregistrées, si vous avez enregistré des requêtes. Pour aider à contrôler les coûts, nous vous recommandons de limiter les requêtes en ajoutant des horodatages `eventTime` de début et de fin aux requêtes.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Requête.
3. Sur la page Requête, sélectionnez l'onglet Exemples de requêtes.
4. Ouvrez un exemple de requête en choisissant le nom de la requête. Cela ouvre la requête dans l'onglet Éditeur. Dans cet exemple, nous allons sélectionner la requête intitulée Investigate user actions et modifier la requête pour trouver les actions d'un utilisateur spécifique nommé `Alice`.
5. Dans l'onglet Éditeur, modifiez la ligne `WHERE` pour spécifier l'utilisateur que vous souhaitez étudier et mettez à jour les valeurs `eventTime` selon les besoins. La valeur de `FROM` est la partie ID de l'ARN du magasin de données d'événements et est automatiquement renseignée CloudTrail lorsque vous choisissez le magasin de données d'événements.

```
SELECT
```

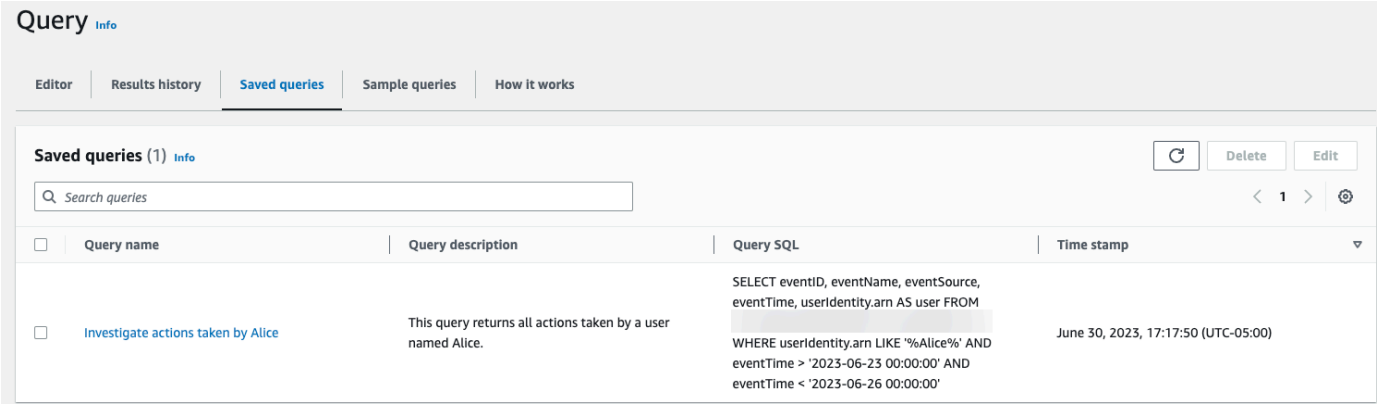
```
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. Vous pouvez exécuter une requête avant de l'enregistrer, pour vérifier que la requête fonctionne. Pour exécuter une requête, choisissez un magasin de données d'événement dans la liste déroulante Event data store (Magasin de données d'événement), puis choisissez Run (Exécuter). Affichez la colonne Statut de l'onglet Sortie de la commande pour la requête active afin de vérifier qu'une requête s'est exécutée correctement.
7. Lorsque vous avez mis à jour l'exemple de requête, choisissez Enregistrer.
8. Dans Enregistrer la requête, saisissez un nom et une description pour la requête. Choisissez Save query (Enregistrer la requête) pour enregistrer vos modifications en tant que nouvelle requête. Pour ignorer les modifications apportées à une requête, choisissez Cancel (Annuler) ou fermez la fenêtre Save query (Enregistrer la requête).



> **Note**
>
> Les requêtes enregistrées sont liées à votre navigateur ; si vous utilisez un autre navigateur ou un autre appareil pour accéder à la CloudTrail console, les requêtes enregistrées ne sont pas disponibles.

9. Ouvrez l'onglet Saved queries (Requêtes enregistrées) pour voir la nouvelle requête dans la table.



Exécuter une requête et enregistrer les résultats

Après avoir choisi ou enregistré une requête, vous pouvez l'exécuter sur un magasin de données d'événement.

Lorsque vous exécutez une requête, vous avez la possibilité d'enregistrer les résultats de la requête dans un compartiment Amazon S3. Lorsque vous exécutez des requêtes dans CloudTrail Lake, des frais sont facturés en fonction de la quantité de données numérisées par la requête. Aucun frais CloudTrail Lake supplémentaire n'est facturé pour l'enregistrement des résultats des requêtes dans un compartiment S3, mais des frais de stockage S3 sont facturés. Pour de plus amples informations sur la tarification S3, veuillez consulter Tarification Amazon S3.

Lorsque vous enregistrez des résultats de requête, ils peuvent s'afficher dans la CloudTrail console avant d'être visibles dans le compartiment S3, car ils sont fournis CloudTrail une fois l'analyse des requêtes terminée. Bien que la plupart des requêtes soient traitées en quelques minutes, selon la taille de votre banque de données d'événements, la transmission des résultats des requêtes CloudTrail à votre compartiment S3 peut prendre beaucoup plus de temps. CloudTrail fournit les résultats de la requête au compartiment S3 au format gzip compressé. En moyenne, une fois

l'analyse de la requête terminée, vous pouvez vous attendre à une latence de 60 à 90 secondes pour chaque Go de données envoyé vers le compartiment S3.

Pour exécuter une requête à l'aide de CloudTrail Lake

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Requête.
3. Dans les onglets Requêtes enregistrées ou Exemples de requêtes, choisissez une requête à exécuter en choisissant le nom de la requête.
4. Dans l'onglet Éditeur, pour Magasin de données d'événement, choisissez un magasin de données d'événement dans la liste déroulante.
5. (Facultatif) Dans l'onglet Editor (Éditeur), choisissez Save results to S3 (Enregistrer les résultats dans S3) pour enregistrer les résultats de la requête dans un compartiment S3. Lorsque vous choisissez le compartiment S3 par défaut, il CloudTrail crée et applique les politiques de compartiment requises. Si vous choisissez le compartiment S3 par défaut, votre politique IAM doit inclure une autorisation pour l'`s3:PutEncryptionConfiguration`action, car le chiffrement côté serveur est activé par défaut pour le compartiment. Pour plus d'informations sur l'enregistrement des résultats d'une requête, consultez Informations supplémentaires sur les résultats enregistrés d'une requête.

   > **Note**
   >
   > Pour utiliser un compartiment différent, indiquez un nom de compartiment ou choisissez Browse S3 (Parcourir S3) pour sélectionner un compartiment. La politique du compartiment doit accorder CloudTrail l'autorisation de fournir les résultats de la requête au compartiment. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake.

6. Dans l'onglet Éditeur, choisissez Exécuter.

   Selon la taille de votre magasin de données d'événement et le nombre de jours de données qu'il inclut, l'exécution d'une requête peut prendre plusieurs minutes. L'onglet Command output (Sortie de la commande) affiche l'état d'une requête, et indique si l'exécution d'une requête est terminée. Lorsque l'exécution d'une requête est terminée, ouvrez l'onglet Résultats des requêtes

pour afficher un tableau des résultats de la requête active (la requête actuellement affichée dans l'éditeur).

> **Note**
>
> Les requêtes qui s'exécutent pendant plus d'une heure peuvent prendre fin. Vous pouvez toujours obtenir des résultats partiels qui ont été traités avant l'expiration du délai imparti pour la requête. CloudTrail ne fournit pas de résultats de requête partiels à un compartiment S3. Pour éviter un dépassement de délai, vous pouvez affiner votre requête pour limiter la quantité de données analysées en spécifiant une plage de temps plus étroite.

Informations supplémentaires sur les résultats enregistrés d'une requête

Après avoir enregistré les résultats d'une requête, vous pouvez les télécharger depuis le compartiment S3. Pour plus d'informations sur la recherche et le téléchargement des résultats enregistrés d'une requête, consultez Téléchargement des résultats enregistrés d'une requête.

Vous pouvez également valider les résultats de requête enregistrés pour déterminer s'ils ont été modifiés, supprimés ou CloudTrail inchangés après leur réception. Pour plus d'informations sur la validation des résultats enregistrés d'une requête, consultez Validation des résultats enregistrés d'une requête.

Exemple : enregistrer les résultats d'une requête dans un compartiment Amazon S3

Cette procédure pas à pas montre comment enregistrer les résultats d'une requête dans un compartiment S3, puis comment les télécharger.

Pour enregistrer les résultats d'une requête dans un compartiment Amazon S3

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Requête.
3. Dans les onglets Requêtes enregistrées ou Exemples de requêtes, choisissez une requête à exécuter en choisissant la valeur dans la colonne SQL de la requête. Dans cet exemple, nous allons choisir l'exemple de requête intitulé Investigate user actions.
4. Dans l'onglet Éditeur, pour Magasin de données d'événement, choisissez un magasin de données d'événement dans la liste déroulante. Lorsque vous choisissez le magasin de

données d'événements dans la liste, l'ID du magasin de données d'événements est CloudTrail automatiquement renseigné dans la `From` ligne.

5. Dans cet exemple de requête, nous allons modifier la valeur `userIdentity.ARN` pour spécifier un utilisateur nommé `Admin`, et nous allons conserver les valeurs par défaut pour `eventTime`. Lorsque vous exécutez une requête, la quantité de données analysées vous est facturée. Pour aider à contrôler les coûts, nous vous recommandons de limiter les requêtes en ajoutant des horodatages `eventTime` de début et de fin aux requêtes.

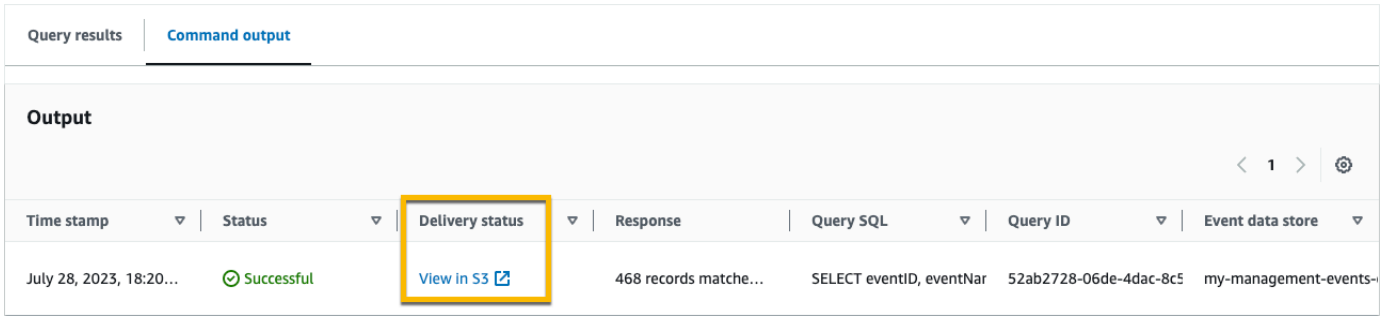
6. Choisissez Enregistrer les résultats dans S3 pour enregistrer les résultats de la requête dans un compartiment S3. Lorsque vous choisissez le compartiment S3 par défaut, il CloudTrail crée et applique les politiques de compartiment requises. Si vous choisissez le compartiment S3 par défaut, votre politique IAM doit inclure une autorisation pour l'`s3:PutEncryptionConfiguration`action, car le chiffrement côté serveur est activé par défaut pour le compartiment. Dans cet exemple, nous utiliserons le compartiment S3 par défaut.

> **Note**
>
> Pour utiliser un compartiment différent, indiquez un nom de compartiment ou choisissez Parcourir S3 pour sélectionner un compartiment. La politique du compartiment doit accorder CloudTrail l'autorisation de fournir les résultats de la requête au compartiment. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake.

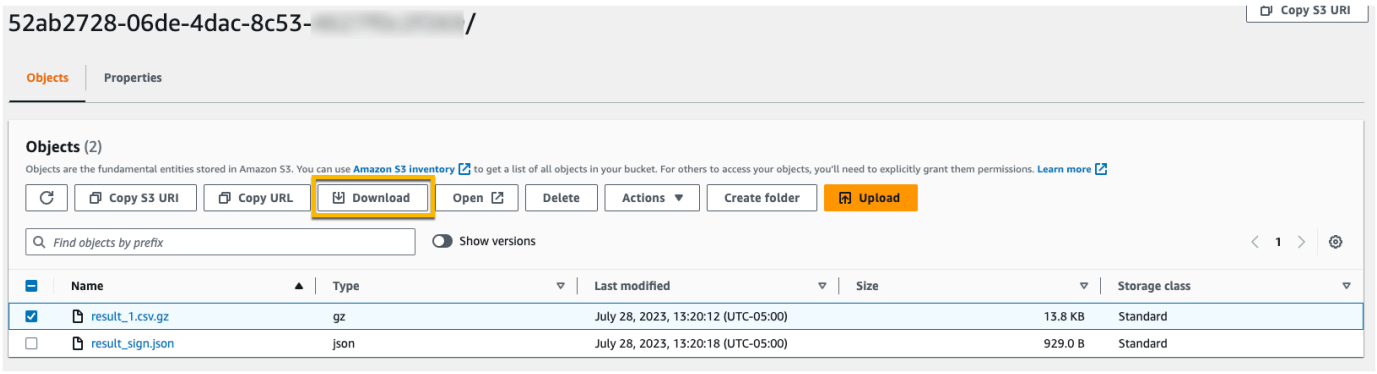
7. Cliquez sur Exécuter. Selon la taille de votre magasin de données d'événement et le nombre de jours de données qu'il inclut, l'exécution d'une requête peut prendre plusieurs minutes. L'onglet Command output (Sortie de la commande) affiche l'état d'une requête, et indique si l'exécution d'une requête est terminée. Lorsque l'exécution d'une requête est terminée, ouvrez l'onglet Résultats des requêtes pour afficher un tableau des résultats de la requête active (la requête actuellement affichée dans l'éditeur).
8. Lorsque la livraison des résultats de requête enregistrés à votre compartiment S3 est CloudTrail terminée, la colonne État de livraison fournit un lien vers le compartiment S3 qui contient vos fichiers de résultats de requête enregistrés ainsi qu'un fichier de signature que vous pouvez utiliser pour vérifier les résultats de vos requêtes enregistrés. Choisissez Afficher dans S3 pour afficher les fichiers de résultats de la requête et les fichiers de signature dans le compartiment S3.

> **Note**
>
> Lorsque vous enregistrez des résultats de requête, ils peuvent s'afficher dans la CloudTrail console avant d'être visibles dans le compartiment S3, car ils sont fournis CloudTrail une fois l'analyse des requêtes terminée. Bien que la plupart des requêtes soient traitées en quelques minutes, selon la taille de votre banque de données d'événements, la transmission des résultats des requêtes CloudTrail à votre compartiment S3 peut prendre beaucoup plus de temps. CloudTrail fournit les résultats de la requête au compartiment S3 au format gzip compressé. En moyenne, une fois

l'analyse de la requête terminée, vous pouvez vous attendre à une latence de 60 à 90 secondes pour chaque Go de données envoyé vers le compartiment S3.



9. Pour télécharger les résultats de votre requête, choisissez le fichier de résultats de la requête (en l'occurrence `result_1.csv.gz`), puis choisissez Télécharger.



Pour plus d'informations sur la validation des résultats enregistrés d'une requête, veuillez consulter Validation des résultats enregistrés d'une requête.

Afficher les résultats des requêtes

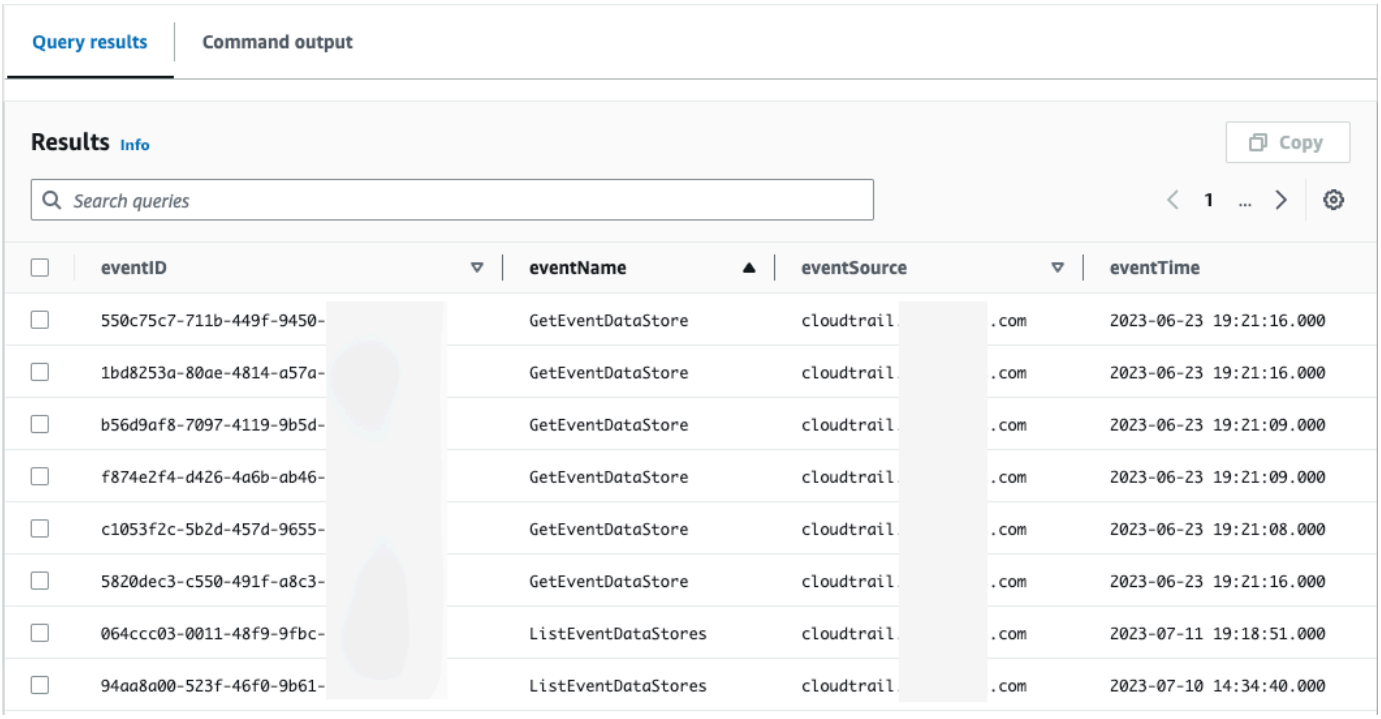
Une fois votre requête terminée, vous pouvez afficher ses résultats. Les résultats d'une requête sont disponibles pendant sept jours après la fin de la requête. Vous pouvez afficher les résultats de la requête active sur l'onglet Query results (Résultats des requêtes), ou vous pouvez accéder aux résultats de toutes les requêtes récentes sur l'onglet Result history (Historique des résultats) sur la page d'accueil Lake.

Les résultats de la requête peuvent passer des exécutions plus anciennes d'une requête à des exécutions plus récentes, car les événements ultérieurs de la période de requête peuvent être journalisés entre les requêtes.

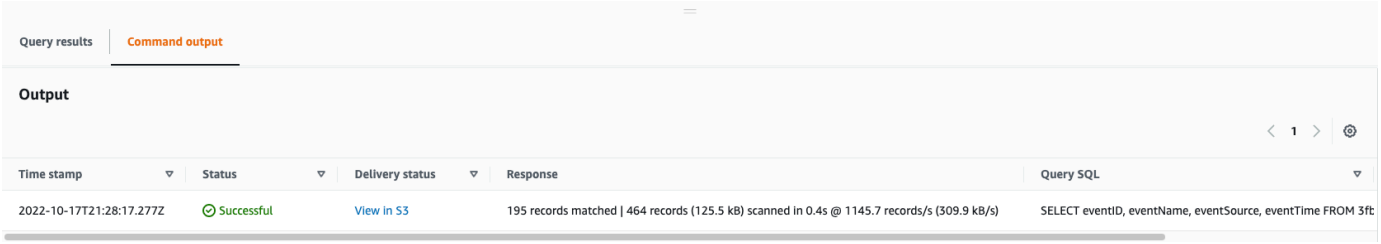
Lorsque vous enregistrez des résultats de requête, ils peuvent s'afficher dans la CloudTrail console avant d'être visibles dans le compartiment S3, car ils sont fournis CloudTrail une fois l'analyse des requêtes terminée. Bien que la plupart des requêtes soient traitées en quelques minutes, selon la taille de votre banque de données d'événements, la transmission des résultats des requêtes CloudTrail à votre compartiment S3 peut prendre beaucoup plus de temps. CloudTrail fournit les résultats de la requête au compartiment S3 au format gzip compressé. En moyenne, une fois l'analyse des requêtes terminée, vous pouvez vous attendre à une latence de 60 à 90 secondes pour chaque Go de données transmis au compartiment S3. Pour plus d'informations sur la recherche et le téléchargement des résultats enregistrés d'une requête, consultez Téléchargement des résultats enregistrés d'une requête.

> **Note**
>
> Les requêtes qui s'exécutent pendant plus d'une heure peuvent prendre fin. Vous pouvez toujours obtenir des résultats partiels qui ont été traités avant l'expiration du délai imparti pour la requête. CloudTrail ne fournit pas de résultats de requête partiels à un compartiment S3. Pour éviter un dépassement de délai, vous pouvez affiner votre requête pour limiter la quantité de données analysées en spécifiant une plage de temps plus étroite.

1. Dans l'onglet Résultats des requêtes pour une requête active, chaque ligne représente un résultat d'événement correspondant à la requête. Filtrez les résultats en saisissant tout ou partie d'une valeur de champ d'événement dans la barre de recherche. Pour copier un événement, choisissez l'événement que vous souhaitez copier, puis choisissez Copier.



2. Dans l'onglet Sortie de la commande, affichez les métadonnées relatives à la requête exécutée, telles que l'ID du magasin de données d'événement, la durée d'exécution, le nombre de résultats analysés et si la requête a réussi ou non. Si vous avez enregistré les résultats d'une requête dans un compartiment Amazon S3, les métadonnées incluent également un lien vers le compartiment S3 contenant les résultats enregistrés de la requête.



Téléchargement des résultats enregistrés d'une requête

Après avoir enregistré les résultats de la requête, vous devez être en mesure de localiser le fichier contenant les résultats de la requête. CloudTrail fournit les résultats de votre requête à un compartiment Amazon S3 que vous spécifiez lorsque vous enregistrez les résultats de la requête.

> **Note**
>
> Lorsque vous enregistrez des résultats de requête, ils peuvent s'afficher dans la console avant d'être visibles dans le compartiment S3, car ils sont fournis CloudTrail une fois l'analyse

des requêtes terminée. Bien que la plupart des requêtes soient traitées en quelques minutes, selon la taille de votre banque de données d'événements, la transmission des résultats des requêtes CloudTrail à votre compartiment S3 peut prendre beaucoup plus de temps. CloudTrail fournit les résultats de la requête au compartiment S3 au format gzip compressé. En moyenne, une fois l'analyse de la requête terminée, vous pouvez vous attendre à une latence de 60 à 90 secondes pour chaque Go de données envoyé vers le compartiment S3.

Rubriques

Trouvez les résultats de vos requêtes enregistrés sur CloudTrail Lake

CloudTrail publie les résultats de la requête et les fichiers de signature dans votre compartiment S3. Le fichier de résultat d'une requête contient la sortie de la requête enregistrée. Le fichier de signature fournit la signature et la valeur de hachage des résultats de la requête. Vous pouvez utiliser le fichier de signature pour valider les résultats de la requête. Pour plus d'informations sur la validation des résultats d'une requête, consultez Validation des résultats enregistrés d'une requête.

Pour récupérer le résultat d'une requête ou le fichier de signature, vous pouvez utiliser la console Amazon S3, l'interface de la ligne de commande (CLI) Amazon S3 ou l'API.

Pour trouver les résultats de votre requête et les fichiers de signature avec la console Amazon S3

1. Ouvrez la console Amazon S3.
2. Choisissez le compartiment que vous avez spécifié.
3. Parcourez la hiérarchie des objets jusqu'à ce que vous trouviez les fichiers de résultat de la requête et les fichiers de signature. Le fichier de résultat d'une requête a une extension .csv.gz et le fichier de signature a une extension .json.

Vous allez parcourir une hiérarchie d'objets similaire à l'exemple suivant, mais avec un nom de compartiment, un ID de compte, une date et un ID de requête différents.

```
All Buckets
    Bucket_Name
```

```
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

Téléchargez les résultats de vos requêtes enregistrés sur CloudTrail Lake

Lorsque vous enregistrez les résultats d'une requête CloudTrail , deux types de fichiers sont envoyés dans votre compartiment Amazon S3.

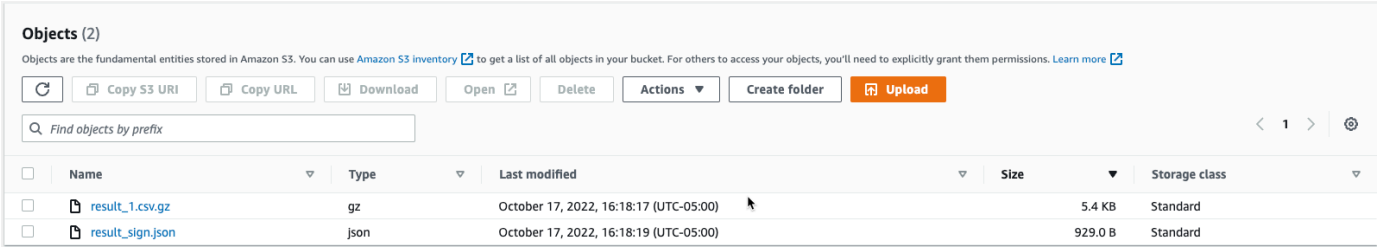
- Un fichier de signature au format JSON que vous pouvez utiliser pour valider les fichiers de résultats de la requête. Le fichier de signature est nommé result_sign.json. Pour plus d'informations sur le fichier de signature, consultez CloudTrail structure du fichier de signes.
- Un ou plusieurs fichiers de résultat au format CSV, qui contiennent les résultats de la requête. Le nombre de fichiers de résultat envoyés dépend de la taille totale des résultats de la requête. La taille maximale d'un fichier de résultat d'une requête est de 1 To. Chaque fichier de résultat d'une requête est nommé result_*number*.csv.gz. Par exemple, si la taille totale des résultats d'une requête était de 2 To, vous auriez deux fichiers de résultat, result_1.csv.gz et result_2.csv.gz.

CloudTrail les fichiers de résultat et de signature de la requête sont des objets Amazon S3. Vous pouvez utiliser la console S3, la AWS Command Line Interface (CLI) ou l'API S3 pour récupérer les résultats des requêtes et signer les fichiers.

La procédure suivante décrit comment télécharger les fichiers de résultat d'une requête et les fichiers de signature avec la console Amazon S3.

Pour télécharger le résultat de votre requête ou le fichier de signature avec la console Amazon S3

1. Ouvrez la console Amazon S3.
2. Choisissez le compartiment et le fichier que vous voulez télécharger.



3. Choisissez Download (Télécharger) et suivez toutes les instructions pour enregistrer le fichier.

> **Note**
>
> Certains navigateurs, tels que Chrome, extraient automatiquement le fichier de résultat de la requête pour vous. Si c'est le cas pour votre navigateur, passez directement à l'étape 5.

4. Utilisez un outil comme 7-Zip pour extraire le fichier de résultat de la requête.
5. Ouvrez le fichier de résultat de la requête ou le fichier de signature.

Validation des résultats enregistrés d'une requête

Pour déterminer si les résultats de la requête ont été modifiés, supprimés ou inchangés après CloudTrail leur réception, vous pouvez utiliser la validation de l'intégrité des résultats de CloudTrail requête. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers de résultats de CloudTrail requêtes sans détection. Vous pouvez utiliser la ligne de commande pour valider les fichiers de résultat d'une requête.

Pourquoi l'utiliser ?

Les fichiers de résultat d'une requête validés s'avèrent utiles lors d'enquêtes de sécurité et légales. Par exemple, un fichier de résultat d'une requête validé vous permet d'affirmer de manière positive que le fichier lui-même n'a pas été modifié. Le processus de validation de l'intégrité du fichier de résultats de CloudTrail requête vous permet également de savoir si un fichier de résultats de requête a été supprimé ou modifié.

Rubriques

- Validez les résultats de requête enregistrés à l'aide du AWS CLI

- CloudTrail structure du fichier de signes
- Implémentations personnalisées de la validation de l'intégrité des fichiers de résultats de CloudTrail requêtes

Validez les résultats de requête enregistrés à l'aide du AWS CLI

Vous pouvez valider l'intégrité des fichiers de résultat d'une requête et du fichier de signature à l'aide de la commande aws cloudtrail verify-query-results.

Prérequis

Pour valider l'intégrité des résultats d'une requête à l'aide de la ligne de commande, les conditions suivantes doivent être remplies :

- Vous devez disposer d'une connexion en ligne pour AWS.
- Vous devez utiliser AWS CLI la version 2.
- Pour valider les fichiers de résultats d'une requête et le fichier de signature localement, les conditions suivantes s'appliquent :
  - Vous devez placer les fichiers de résultats d'une requête et le fichier de signature dans le chemin d'accès spécifié. Indiquez le chemin d'accès au fichier comme valeur du paramètre --local-export-path.
  - Ne renommez ni les fichiers de résultats d'une requête, ni le fichier de signature.
- Pour valider les fichiers de résultats d'une requête et le fichier de signature dans le compartiment S3, les conditions suivantes s'appliquent :
  - Ne renommez ni les fichiers de résultats d'une requête, ni le fichier de signature.
  - Vous devez disposer d'un accès en lecture au compartiment Amazon S3 qui contient les fichiers de résultat d'une requête et le fichier de signature.
  - Le préfixe S3 spécifié doit contenir les fichiers de résultats d'une requête et le fichier de signature. Spécifiez le préfixe S3 comme valeur du paramètre --s3-prefix.

verify-query-results

La commande verify-query-results vérifie la valeur de hachage de chaque fichier de résultats d'une requête `fileHashValue` en la comparant à la valeur du fichier de signature, puis en validant `hashSignature` dans le fichier de signature.

Lorsque vous vérifiez les résultats d'une requête, vous pouvez utiliser les options de ligne de commande --s3-bucket et --s3-prefix pour valider les fichiers de résultats d'une requête et le fichier de signature stockés dans un compartiment S3, ou vous pouvez utiliser l'option de ligne de commande --local-export-path pour effectuer une validation locale des fichiers de résultats d'une requête et du fichier de signature téléchargés.

> **Note**
>
> La commande verify-query-results est spécifique à la région. Vous devez spécifier l'option --region globale pour valider les résultats d'une requête spécifique Région AWS.

Voici les options pour la commande verify-query-results.

--s3-bucket *<string>*

Spécifie le nom du compartiment S3 qui stocke les fichiers de résultats d'une requête et le fichier de signature. Vous ne pouvez pas utiliser ce paramètre avec --local-export-path.

--s3-prefix *<string>*

Spécifie le chemin S3 du dossier S3 qui contient les fichiers de résultats d'une requête et le fichier de signature (par exemple, `s3/path/`). Vous ne pouvez pas utiliser ce paramètre avec --local-export-path. Il n'est pas nécessaire de fournir ce paramètre si les fichiers se trouvent dans le répertoire racine du compartiment S3.

--local-export-path *<string>*

Spécifie le répertoire local qui contient les fichiers de résultats d'une requête et le fichier de signature (par exemple, `/local/path/to/export/file/`). Vous ne pouvez pas utiliser ce paramètre avec --s3-bucket ou --s3-prefix.

Exemples

L'exemple suivant valide les résultats d'une requête à l'aide des options de ligne de commande --s3-bucket et --s3-prefix pour spécifier le nom du compartiment S3 et le préfixe contenant les fichiers de résultats d'une requête et le fichier de signature.

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

L'exemple suivant valide les résultats d'une requête téléchargés en utilisant l'option de ligne de commande --local-export-path pour spécifier le chemin local pour les fichiers de résultats d'une requête et le fichier de signature. Pour plus d'informations sur le téléchargement des résultats d'une requête, veuillez consulter Téléchargez les résultats de vos requêtes enregistrés sur CloudTrail Lake.

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

Résultats de la validation

Le tableau suivant décrit les messages de validation possibles pour les fichiers de résultats d'une requête et le fichier de signature.

Type de fichier	Message de validation	Description
`Sign file`	`Successfully validated sign and query result files`	La signature du fichier de signature est valide. Les fichiers de résultats d'une requête auxquels il fait référence peuvent être vérifiés.
`Query result file`	`ValidationError: "File` *`file_name`* `has inconsistent hash value with hash value recorded in sign file, hash value in sign file is` *`expected_hash`* `, but get` *`computed_hash`*	La validation a échoué, car la valeur de hachage du fichier de résultats d'une requête ne correspondait pas au `fileHashValue` dans le fichier de signature.
`Sign file`	`ValidationError: Invalid signature in sign file`	La validation du fichier de signature a échoué, car la signature n'est pas valide.

CloudTrail structure du fichier de signes

Le fichier de signature contient le nom de chaque fichier de résultat d'une requête qui a été envoyé à votre compartiment Amazon S3 lorsque vous avez enregistré les résultats d'une requête, la valeur de hachage de chaque fichier de résultat de la requête et la signature numérique du fichier. La signature numérique et les valeurs de hachage sont utilisées pour valider l'intégrité des fichiers de résultat de la requête et du fichier de signature lui-même.

Emplacement du fichier de signature

Le fichier de signature est envoyé à un emplacement de compartiment Amazon S3 qui respecte cette syntaxe.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

Exemple de contenu du fichier de signature

L'exemple de fichier de signes suivant contient des informations relatives aux résultats des requêtes CloudTrail Lake.

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

Description des champs du fichier de signature

Voici la description de chaque champ du fichier de signature :

`version`

La version du fichier de signature.

`region`

Région du AWS compte utilisé pour enregistrer les résultats de la requête.

`files.fileHashValue`

La valeur de hachage codée en hexadécimal du contenu compressé du fichier de résultat de la requête.

`files.fileName`

Le nom du fichier de resultat de la requête.

`hashAlgorithm`

L'algorithme de hachage utilisé pour hacher le fichier de résultat de la requête.

`signatureAlgorithm`

L'algorithme utilisé pour signer le fichier.

`queryCompleteTime`

Indique à CloudTrail quel moment les résultats de la requête ont été transmis au compartiment S3. Vous pouvez utiliser cette valeur pour trouver la clé publique.

`hashSignature`

La signature de hachage du fichier.

`publicKeyFingerprint`

L'empreinte digitale codée en hexadécimal de la clé publique utilisée pour signer le fichier.

Implémentations personnalisées de la validation de l'intégrité des fichiers de résultats de CloudTrail requêtes

Grâce à l' CloudTrail utilisation d'algorithmes cryptographiques et de fonctions de hachage conformes aux normes du secteur et librement disponibles, vous pouvez créer vos propres outils pour valider l'intégrité des fichiers de résultats des CloudTrail requêtes. Lorsque vous enregistrez les résultats d'une requête dans un compartiment Amazon S3, CloudTrail un fichier de signature est envoyé à votre compartiment S3. Vous pouvez mettre en œuvre votre propre solution de validation pour valider les fichiers de signature et les fichiers de résultats d'une requête. Pour plus d'informations sur le fichier de signature, consultez CloudTrail structure du fichier de signes.

Cette rubrique décrit comment le fichier de signature est signé, puis détaille les étapes que vous devrez suivre pour mettre en œuvre une solution qui valide le fichier de signature et les fichiers de résultat d'une requête auxquels le fichier de signature fait référence.

Comprendre comment CloudTrail les fichiers de signature sont signés

CloudTrail les fichiers de signature sont signés avec des signatures numériques RSA. Pour chaque fichier de signes, CloudTrail effectue les opérations suivantes :

1. Crée une liste de hachage qui contient la valeur de hachage de chaque fichier de résultat d'une requête.
2. Obtient une clé privée unique pour la région.
3. Transmet le hachage SHA-256 de la chaîne et la clé privée de l'algorithme de signature RSA, qui génèrent une signature numérique.
4. Code le code d'octet de la signature dans un format hexadécimal.
5. Ajoute la signature numérique dans le fichier de signature.

Contenu de la chaîne de signature des données

La chaîne de signature des données est constituée de la valeur de hachage de chaque fichier de résultat d'une requête, séparés par un espace. Le fichier de signature énumère la valeur `fileHashValue` de chaque fichier de résultat d'une requête.

Étapes d'implémentation de la validation personnalisée

Lors de la mise en œuvre d'une solution de validation personnalisée, vous devrez valider le fichier de signature et les fichiers de résultat d'une requête auxquels il fait référence.

Validation du fichier de signature

Pour valider un fichier de signature, vous avez besoin de sa signature, de la clé publique dont la clé privée a été utilisée pour le signer et d'une chaîne de signature de données que vous calculez.

1. Obtenir le fichier de signature.
2. Vérifier que le fichier de signature a été récupéré depuis son emplacement d'origine.
3. Obtenir la signature codée en hexadécimal du fichier de signature.
4. Obtenir l'empreinte digitale codée en hexadécimal de la clé publique dont la clé privée a été utilisée pour signer le fichier de signature.
5. Récupérer la clé publique pour la plage de temps correspondant à `queryCompleteTime` dans le fichier de signature. Pour la plage de temps, choisissez une `StartTime` antérieure à la `queryCompleteTime` et une `EndTime` postérieure à la `queryCompleteTime`.
6. Parmi les clés publiques récupérées, choisissez la clé publique dont l'empreinte digitale correspond à la valeur `publicKeyFingerprint` dans le fichier de signature.
7. À l'aide d'une liste de hachage contenant la valeur de hachage de chaque fichier de résultat d'une requête séparées par un espace, recréez la chaîne de signature des données utilisée pour vérifier la signature du fichier de signature. Le fichier de signature énumère la valeur `fileHashValue` de chaque fichier de résultat d'une requête.

   Par exemple, si le tableau `files` de votre fichier de signature contient les trois fichiers de résultat d'une requête suivants, votre liste de hachage est « aaa bbb ccc ».

```
“files": [

   {

        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"

   },
   {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

   },
```

```
    {

         "fileHashValue" : “ccc”,

         "fileName" : "result_3.csv.gz"

    }
],
```

8. Valider la signature en transmettant le hachage SHA-256 de la chaîne, la clé publique et la signature comme paramètres de l'algorithme de vérification de signature RSA. Si le résultat est true, le fichier de signature est valide.

Validation des fichiers de résultat d'une requête

Si le fichier de signature est valide, validez les fichiers de résultat d'une requête auxquels le fichier de signature fait référence. Pour valider l'intégrité d'un fichier de résultat d'une requête, calculez sa valeur de hachage SHA-256 sur son contenu compressé et comparez les résultats avec la valeur `fileHashValue` du fichier de résultat d'une requête enregistrée dans le fichier de signature. Si les hachages correspondent, le fichier de résultat de la requête est valide.

Les sections suivantes décrivent en détail le processus de validation.

A. Obtenir le fichier de signature

Les premières étapes consistent à obtenir le fichier de signature et l'empreinte digitale de la clé publique.

1. Obtenez le fichier de signature à partir de votre compartiment Amazon S3 pour les résultats de la requête que vous voulez valider.
2. Ensuite, obtenez la valeur `hashSignature` à partir du fichier de signature.
3. Dans le fichier de signature, obtenez l'empreinte digitale de la clé publique dont la clé privée a été utilisée pour signer le fichier à partir du champ `publicKeyFingerprint`.

B. Récupérer la clé publique pour valider le fichier de signature

Pour obtenir la clé publique permettant de valider le fichier de signature, vous pouvez utiliser l'API AWS CLI ou l' CloudTrail API. Dans les deux cas, vous spécifiez une plage de temps (c'est-à-dire, une heure de début et une heure de fin) pour le fichier de signature que vous voulez valider. Utilisez une plage horaire correspondant à la `queryCompleteTime` dans le fichier de signature. Une ou

plusieurs clés publiques peuvent être retournées pour l'intervalle de temps que vous spécifiez. Les clés renvoyées peuvent avoir des plages de temps de validité qui se chevauchent.

> **Note**
>
> Comme il CloudTrail utilise différentes paires de clés publiques/privées par région, chaque fichier de signes est signé avec une clé privée propre à sa région. Par conséquent, lorsque vous validez un fichier de signature à partir d'une région donnée, vous devez récupérer sa clé publique à partir de la même région.

Utilisez le AWS CLI pour récupérer les clés publiques

Pour récupérer une clé publique pour un fichier de signes à l'aide de AWS CLI, utilisez la `cloudtrail list-public-keys` commande. La commande a le format suivant :

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Les paramètres d'heure de début et d'heure de fin sont des horodatages UTC facultatifs. S'ils ne sont pas spécifiés, l'heure actuelle est utilisée et la ou les clés publiques actives sont renvoyées.

Exemple de réponse

La réponse est une liste d'objets JSON représentant la (ou les) clé(s) renvoyées :

Utiliser l' CloudTrail API pour récupérer les clés publiques

Pour récupérer une clé publique pour un fichier de signes à l'aide de l' CloudTrail API, transmettez les valeurs d'heure de début et de fin à l'`ListPublicKeys`API. L'API `ListPublicKeys` renvoie les clés publiques dont les clés privées ont été utilisées pour signer le fichier dans la plage de temps spécifiée. Pour chaque clé publique, l'API renvoie également l'empreinte correspondante.

`ListPublicKeys`

Cette section décrit les paramètres de demande et les éléments de réponse pour l'API `ListPublicKeys`.

> **Note**
>
> L'encodage pour les champs binaires pour `ListPublicKeys` est susceptible d'être modifié.

Paramètres de requête

Name (Nom)	Description
`StartTime`	Spécifie éventuellement, en UTC, le début de la plage de temps pour rechercher la clé publique pour le fichier de CloudTrail signature. Si StartTime ce n'est pas spécifié, l'heure actuelle est utilisée et la clé publique actuelle est renvoyée. Type : DateTime
`EndTime`	Spécifie éventuellement, en UTC, la fin de la plage de temps pour rechercher les clés publiques pour les fichiers de CloudTrail signature. Si EndTime ce n'est pas spécifié, l'heure actuelle est utilisée. Type : DateTime

Éléments de réponse

`PublicKeyList`, un tableau des objets `PublicKey` qui contient les éléments suivants :

Name (Nom)	Description
`Value`	La valeur de clé publique codée DER au format PKCS #1. Type : Blob
`ValidityStartTime`	Heure de début de validité de la clé publique. Type : DateTime
`ValidityEndTime`	Heure de fin de validité de la clé publique. Type : DateTime
`Fingerprint`	Empreinte de la clé publique. L'empreinte peut servir à identifier la clé publique que vous devez utiliser pour valider le fichier de signature. Type : chaîne

C. Sélectionner la clé publique à utiliser pour la validation

Parmi les clés publiques récupérées par `list-public-keys` ou `ListPublicKeys`, sélectionnez la clé publique dont l'empreinte digitale correspond à l'empreinte digitale enregistrée dans le champ `publicKeyFingerprint` du fichier de signature. C'est la clé publique que vous utiliserez pour valider le fichier de signature.

D. Recréer la chaîne de signature des données

Maintenant que vous avez la signature du fichier de signature et la clé publique associée, vous devez calculer la chaîne de signature des données. Une fois que vous aurez calculé les chaîne de signature des données, vous aurez les entrées nécessaires pour vérifier la signature.

La chaîne de signature des données est constituée de la valeur de hachage de chaque fichier de résultat d'une requête, séparés par un espace. Une fois que vous avez recréé cette chaîne, vous pouvez valider le fichier de signature.

E. Validation du fichier de signature

Transmettez la chaîne de signature de données recréée, la signature numérique et la clé publique de l'algorithme de vérification de la signature RSA. Si le résultat est true, la signature du fichier de signature est vérifiée et le fichier de signature est valide.

F. Validation des fichiers de résultat d'une requête

Une fois que vous avez validé le fichier signature, vous pouvez valider les fichiers de résultat de la requête auxquels il fait référence. Le fichier de signature contient les hachages SHA-256 des fichiers de résultat d'une requête. Si l'un des fichiers de résultats de requête a été modifié après l'avoir CloudTrail livré, les hachages SHA-256 seront modifiés et la signature du fichier de signature ne correspondra pas.

Utilisez la procédure suivante pour valider les fichiers de résultat d'une requête répertoriés dans le tableau `files` du fichier de signature.

1. Récupérez le hachage original du fichier dans le champ `files.fileHashValue` du fichier de signature.
2. Hachez le contenu compressé du fichier de résultat d'une requête avec l'algorithme de hachage spécifié dans `hashAlgorithm`.
3. Comparez la valeur de hachage que vous avez générée pour chaque fichier de résultat de la requête avec la valeur `files.fileHashValue` du fichier de signature. Si les hachages correspondent, les fichiers de résultat de la requête sont valides.

Validation des fichiers de signature et de résultat d'une requête hors ligne

Lors de la validation des fichiers de signature et des fichiers de résultats d'une requête hors connexion, vous pouvez généralement suivre les procédures décrites dans les sections précédentes. Cependant, vous devez prendre en compte les informations suivantes concernant les clés publiques.

Clés publiques

Pour effectuer une validation hors ligne, la clé publique dont vous avez besoin pour valider les fichiers de résultat d'une requête dans une plage de temps donnée doit d'abord être obtenue en ligne (en appelant `ListPublicKeys`, par exemple), puis stockée hors ligne. Cette étape doit être répétée chaque fois que vous souhaitez valider des fichiers supplémentaires en dehors de la plage de temps que vous avez spécifiée au départ.

Extrait de code de validation

L'exemple d'extrait suivant fournit un code squelette pour valider les fichiers de résultats de CloudTrail signes et de requêtes. Ce squelette de code peut aussi bien être implémenter avec ou sans connexion à AWS ; c'est à vous de décider. L'implémentation suggéré utilise le Java Cryptography Extension (JCE) et Bouncy Castle comme fournisseur de sécurité.

L'exemple d'extrait de code montre :

- Procédure de création de la chaîne de signature des données utilisée pour valider la signature du fichier de signature.
- Procédure de vérification de la signature du fichier de signature.
- Procédure de calcul de la valeur de hachage pour le fichier de résultat d'une requête et comparaison avec la valeur `fileHashValue` répertoriée dans le fichier de signature pour vérifier l'authenticité du fichier de résultat d'une requête.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
```

```
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
 file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
 copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
 fileS3ObjectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
```

```
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                        s3Bucket, fileS3ObjectKey,
                        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                        s3Bucket, fileS3ObjectKey));
            }

            hashList.add(file.getString("fileHashValue"));
        }
        String hashListString = hashList.stream().collect(Collectors.joining(" "));

        /*
            NOTE:
            To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
            of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
            returned from ListPublicKey API are DER encoded in PKCS#1 format:

            PublicKeyInfo ::= SEQUENCE {
                algorithm       AlgorithmIdentifier,
                PublicKey       BIT STRING
            }

            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
rsaPublicKey);
```

```
        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

Exécutez et gérez les requêtes CloudTrail Lake à l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour exécuter et gérer vos requêtes CloudTrail Lake. Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la Région AWS configuration adaptée à votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

Commandes disponibles pour les requêtes CloudTrail Lake

Les commandes permettant d'exécuter et de gérer les requêtes dans CloudTrail Lake incluent :

- `start-query`pour exécuter une requête.
- `describe-query`pour renvoyer des métadonnées relatives à une requête.
- `get-query-results`pour renvoyer les résultats de la requête pour l'ID de requête spécifié.
- `list-queries`pour obtenir une liste de requêtes pour le magasin de données d'événements spécifié.
- `cancel-query`pour annuler une requête en cours d'exécution.

Pour obtenir la liste des commandes disponibles pour les magasins de données d'événements CloudTrail Lake, consultezCommandes disponibles pour les magasins de données d'événements.

Pour obtenir la liste des commandes disponibles pour les intégrations de CloudTrail Lake, consultezCommandes disponibles pour les intégrations de CloudTrail Lake.

Lancez une requête avec AWS CLI

L'exemple de AWS CLI start-query commande suivant exécute une requête sur le magasin de données d'événements spécifié sous forme d'ID dans l'instruction de requête et fournit les résultats de la requête à un compartiment S3 spécifié. Le paramètre `--query-statement` fournit une requête SQL, entre guillemets simples. Les paramètres facultatifs incluent `--delivery-s3uri`, pour envoyer les résultats d'une requête à un compartiment S3 spécifié. Pour plus d'informations sur le langage de requête que vous pouvez utiliser dans CloudTrail Lake, consultezCloudTrail Contraintes SQL du lac.

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

La réponse est une chaîne `QueryId`. Pour obtenir le statut d'une requête, exécutez describe-query en utilisant la valeur `QueryId` renvoyée par start-query. Si la requête est réussie, vous pouvez exécuter get-query-results pour obtenir des résultats.

Sortie

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Les requêtes qui s'exécutent pendant plus d'une heure peuvent prendre fin. Vous pouvez toujours obtenir des résultats partiels traités avant l'échéance de la requête.
> Si vous transmettez les résultats de la requête à un compartiment S3 à l'aide du `--delivery-s3uri` paramètre facultatif, la politique du compartiment doit CloudTrail autoriser la livraison des résultats de la requête au compartiment. Pour en savoir plus sur

la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake.

Obtenez les métadonnées relatives à une requête à l'aide du AWS CLI

L'exemple de AWS CLI describe-query commande suivant permet d'obtenir les métadonnées relatives à une requête, notamment le temps d'exécution de la requête en millisecondes, le nombre d'événements analysés et mis en correspondance, le nombre total d'octets analysés et le statut de la requête. La valeur `BytesScanned` correspond au nombre d'octets pour lesquels votre compte est facturé pour la requête, sauf si la requête est toujours en cours d'exécution. Si les résultats de la requête ont été transmis à un compartiment S3, la réponse fournit également l'URI S3 et le statut de livraison.

Vous devez spécifier une valeur pour le paramètre `--query-id` ou pour le paramètre `--query-alias`. La spécification du paramètre `--query-alias` renvoie des informations sur la dernière requête exécutée pour l'alias.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Voici un exemple de réponse.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

Obtenez les résultats de vos requêtes à l'aide du AWS CLI

L'exemple de commande AWS CLI get-query-results suivant montre comment obtenir les résultats des données d'événement d'une requête. Vous devez spécifier le `--query-id` renvoyé par la

commande start-query. La valeur `BytesScanned` correspond au nombre d'octets pour lesquels votre compte est facturé pour la requête, sauf si la requête est toujours en cours d'exécution. Les paramètres facultatifs incluent `--max-query-results`, pour spécifier un nombre maximal de résultats que la commande doit renvoyer sur une seule page. S'il y a plus de résultats que la valeur `--max-query-results` spécifiée, exécutez à nouveau la commande en ajoutant la valeur `NextToken` renvoyée pour obtenir la page suivante de résultats.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Sortie

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

Répertoriez toutes les requêtes sur un magasin de données d'événements à l'aide du AWS CLI

L'exemple de commande AWS CLI list-queries suivant montre comment renvoyer une liste de requêtes et d'états de requête sur un magasin de données d'événement spécifié au cours des sept derniers jours. Vous devez spécifier un ARN ou le suffixe d'ID d'une valeur ARN pour `--event-data-store`. Pour raccourcir la liste des résultats, vous pouvez également spécifier une plage de temps, formatée en horodatage, en ajoutant les paramètres `--start-time` et `--end-time`, et

une valeur `--query-status`. Les valeurs valides pour `QueryStatus` incluent `QUEUED`, `RUNNING`, `FINISHED`, `FAILED` ou `CANCELLED`.

list-queries dispose également de paramètres de pagination facultatifs. Utilisez `--max-results` pour spécifier un nombre maximal de résultats que la commande doit renvoyer sur une seule page. S'il y a plus de résultats que la valeur `--max-results` spécifiée, exécutez à nouveau la commande en ajoutant la valeur `NextToken` renvoyée pour obtenir la page suivante de résultats.

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

Sortie

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
    "NextToken": "20add42078135EXAMPLE"
}
```

Annulez une requête en cours à l'aide du AWS CLI

L'exemple de AWS CLI cancel-query commande suivant annule une requête dont le statut est. `RUNNING` Vous devez spécifier une valeur pour `--query-id`. Lorsque vous exécutez cancel-query, l'état de la requête peut être `CANCELLED` même si l'opération cancel-query n'est pas encore terminée.

> **Note**
>
> Une requête annulée peut entraîner des frais. Votre compte est toujours facturé pour la quantité de données analysées avant l'annulation de la requête.

Voici un exemple de CLI.

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Sortie

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail Contraintes SQL du lac

CloudTrail Les requêtes Lake sont des chaînes SQL. Cette section fournit des informations sur les fonctions, les opérateurs et les schémas pris en charge.

Seules les instructions `SELECT` sont autorisées. Aucune chaîne de requête ne peut modifier ou muter les données.

CloudTrail Lake prend en charge toutes les `SELECT` instructions, fonctions et opérateurs Presto SQL valides. Pour plus d'informations sur les fonctions et opérateurs SQL pris en charge, veuillez consulter Functions and Operators sur le site Web de documentation de Presto.

La CloudTrail console fournit un certain nombre d'exemples de requêtes qui peuvent vous aider à commencer à écrire vos propres requêtes. Pour plus d'informations, consultez Afficher des exemples de requêtes dans la CloudTrail console.

Rubriques

- Fonctions et opérateurs de condition et de jointure pris en charge
- Prise en charge avancée des requêtes multitables

Fonctions et opérateurs de condition et de jointure pris en charge

Fonctions prises en charge

CloudTrail Lake prend en charge toutes les fonctions Presto. Pour plus d'informations sur les fonctions prises en charge, veuillez consulter Functions and Operators sur le site Web de documentation de Presto.

CloudTrail Lake ne supporte pas le `INTERVAL` mot clé.

Opérateurs de conditions pris en charge

Les opérateurs de condition suivants sont pris en charge.

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

Opérateurs de jointure pris en charge

Les opérateurs `JOIN` suivants sont pris en charge. Pour plus d'informations sur l'exécution de requêtes multitables, consultez Prise en charge avancée des requêtes multitables.

```
UNION
UNION ALL
EXCEPT
INTERSECT
```

```
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

Prise en charge avancée des requêtes multitables

CloudTrail Lake prend en charge le langage de requête avancé dans plusieurs magasins de données d'événements.

- `UNION|UNION ALL|EXCEPT|INTERSECT`
- `LEFT|RIGHT|INNER JOIN`

Pour exécuter votre requête, utilisez la commande start-query de l' AWS CLI. Voici un exemple utilisant l'une des requêtes types de cette section.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

La réponse est une chaîne `QueryId`. Pour obtenir le statut d'une requête, exécutez `describe-query` en utilisant la valeur `QueryId` renvoyée par `start-query`. Si la requête est réussie, vous pouvez exécuter `get-query-results` pour obtenir des résultats.

`UNION|UNION ALL|EXCEPT|INTERSECT`

Voici un exemple de requête qui utilise `UNION` et `UNION ALL` pour trouver des événements par leur ID et leur nom dans trois magasins de données d'événement, EDS1, EDS2 et EDS3. Les résultats sont d'abord sélectionnés dans chaque magasin de données d'événement, puis concaténés, triés par ID d'événement et limités à dix événements.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

LEFT|RIGHT|INNER JOIN

Voici un exemple de requête qui utilise `LEFT JOIN` pour trouver tous les événements d'un magasin de données d'événement nommé `eds2`, mappé sur `edsB`, qui correspondent à ceux d'un magasin de données d'événement principal (à gauche), `edsA`. Les événements retournés se sont produits au plus tard le 1er janvier 2020, et seuls les noms des événements sont retournés.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

Schémas SQL pris en charge pour les entrepôts de données d'événement

Les sections suivantes présentent le schéma SQL pris en charge pour chaque type d'entrepôt de données d'événement.

Rubriques

- Schéma pris en charge pour les CloudTrail champs d'enregistrement d'événements
- Schéma pris en charge pour les champs d'enregistrement d'événements CloudTrail Insights
- Schéma pris en charge pour les champs d'enregistrement des éléments de configuration AWS Config
- Schéma pris en charge pour les AWS Audit Manager champs d'enregistrement des preuves
- Schéma pris en charge pour les champs autres que les AWS événements

Schéma pris en charge pour les CloudTrail champs d'enregistrement d'événements

Voici le schéma SQL valide pour les champs de CloudTrail gestion et d'enregistrement des événements de données. Pour plus d'informations sur les champs CloudTrail d'enregistrement d'événements, consultezCloudTrail enregistrer le contenu.

```
[
```

```
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
"struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
                ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
    {
        "Name": "eventname",
        "Type": "string"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
        "Type": "string"
    },
    {
        "Name": "errorcode",
```

```
        "Type": "string"
    },
    {
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
"array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
```

```
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
"struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
```

```
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsonchecksum",
        "Type": "string"
    }
]
```

Schéma pris en charge pour les champs d'enregistrement d'événements CloudTrail Insights

Voici le schéma SQL valide pour les champs d'enregistrement d'événement Insights. Pour les événements Insights, la valeur de `eventcategory` est `Insight` et la valeur de `eventtype` est `AwsCloudTrailInsight`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
```

```
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type":
"struct<baselineaverage:double,insightaverage:double,baselineduration:integer,
```

```
 insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
                insightaverage:double,baselinevalue:string,baselineaverage:double>>"
    }
]
```

Schéma pris en charge pour les champs d'enregistrement des éléments de configuration AWS Config

Voici le schéma SQL valide pour les champs d'enregistrement des éléments de configuration. Pour les éléments de configuration, la valeur de `eventcategory` est `ConfigurationItem` et la valeur de `eventtype` est `AwsConfigurationItem`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
```

```
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

Schéma pris en charge pour les AWS Audit Manager champs d'enregistrement des preuves

Voici le schéma SQL valide pour les champs d'enregistrement de preuves d'Audit Manager. Pour les champs d'enregistrement des preuves d'Audit Manager, la valeur de `eventcategory` est `Evidence` et la valeur de `eventtype` est `AwsAuditManagerEvidence`. Pour plus d'informations sur l'agrégation des preuves dans CloudTrail Lake à l'aide d'Audit Manager, voir Evidence Finder dans le guide de AWS Audit Manager l'utilisateur.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
```

```
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                 evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

Schéma pris en charge pour les champs autres que les AWS événements

Le schéma SQL valide pour les AWS non-événements est le suivant. Pour les AWS non-événements, la valeur de `eventcategory` is `ActivityAuditLog` et la valeur de `eventtype` is`ActivityLog`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,
```

```
 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

Contrôle des autorisations utilisateur pour CloudTrail Lake

AWS CloudTrail s'intègre à AWS Identity and Access Management (IAM) pour vous aider à contrôler l'accès au CloudTrail lac et aux autres AWS ressources nécessaires CloudTrail . Vous pouvez utiliser IAM pour contrôler quels AWS utilisateurs peuvent créer, configurer ou supprimer des magasins de données d' CloudTrail événements, ou des canaux, démarrer et arrêter l'ingestion d'événements et copier des événements de suivi. Pour en savoir plus, veuillez consulter la section Identity and Access Management pour AWS CloudTrail.

Les rubriques suivantes vous aident à comprendre les autorisations, les politiques et CloudTrail la sécurité :

- Octroi d'autorisations pour CloudTrail l'administration
- Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake
- Autorisations requises pour copier les événements de journal de suivi
- Autorisations nécessaires pour la fédération
- Exemple de politique qui restreint l'accès à un entrepôt de données d'événement basé sur des identifications : Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications
- AWS CloudTrail exemples de politiques basées sur les ressources
- Autorisations requises pour attribuer un administrateur délégué
- Politique de clé KMS par défaut pour les magasins de données d'événements CloudTrail Lake

Gestion des coûts CloudTrail du lac

AWS CloudTrail Les stockages et requêtes de données sur les événements de Lake sont payants. À titre de bonne pratique, nous vous recommandons d'utiliser Services AWS des outils qui peuvent vous aider à gérer les CloudTrail coûts. Vous pouvez également configurer les magasins de données

d'événement de manière à capturer les données dont vous avez besoin tout en conservant un bon rapport coût-efficacité. Pour plus d'informations sur la tarification CloudTrail , consultez Tarification AWS CloudTrail.

Rubriques

Options de tarification du magasin de données d'événement

Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement.

Le tableau suivant décrit les options de tarification disponibles. Le tableau indique l'option Tarification dans la console et la valeur `BillingMode` correspondante pour l'API, et répertorie les périodes de conservation par défaut et maximale pour chaque option.

Option de tarification (console)	BillingMode (API)	Description
Tarification de rétention extensible d'un an	`EXTENDABLE_RETENTION_PRICING`	Recommandé si vous prévoyez d'ingérer moins de 25 To de données d'événement par mois et souhaitez une période de conservation flexible allant jusqu'à 10 ans. Cette option est également recommandée si votre magasin de données d'événement collecte des éléments de configuration AWS Config , des preuves Audit Manager et des événements externes à AWS. Pendant les 366 premiers jours (période de conservation par défaut), le stockage est

Option de tarification (console)	BillingMode (API)	Description
		inclus sans frais supplémentaires dans le prix d'ingestion. Après 366 jours, la rétention prolongée est disponible moyennant un pay-as-you-go prix. Il s'agit de l'option par défaut. Période de conservation par défaut : 366 jours. Période de conservation maximale : 3 653 jours
Tarification de conservation sur sept ans	`FIXED_RETENTION_PRICING`	Recommandé si vous prévoyez d'ingérer plus de 25 To de données sur les événements par mois et si vous avez besoin d'une période de conservation allant jusqu'à 7 ans. La conservation est incluse dans le prix d'ingestion sans frais supplémentaires. Période de conservation par défaut : 2 557 jours. Période de conservation maximale : 2 557 jours

Comprendre les redevances liées CloudTrail au lac

Les tableaux suivants fournissent des informations sur la manière dont les données d'événements CloudTrail Lake sont stockées et les requêtes sont facturées. Pour plus d'informations sur la tarification CloudTrail , consultez Tarification AWS CloudTrail.

Type de frais	Comment vous engagez les frais
Ingestion de données (données non compressées)	Pour CloudTrail Lake, vous payez en fonction des données non compressées ingérées. L'option tarifaire pour le magasin

Type de frais	Comment vous engagez les frais
	de données d'événement détermine le coût d'ingestion des événements : • Tarif de rétention extensible d'un an : propose des tarifs d'ingestion basés sur le type d'événement. • Tarification de rétention sur sept ans : propose des tarifs d'ingestion basés sur le volume de données ingérées. Les économies les plus importantes sont réalisées lorsque le volume de données ingéré par mois dépasse 25 To. Copier des événements de journal de suivi Lorsque vous copiez des événements de suivi dans CloudTrail Lake, CloudTrail décompressez les journaux stockés au format gzip (compressé). CloudTrail Copie ensuite les événements contenus dans les journaux dans votre banque de données d'événements. La taille des données non compressées peut être supérieure à la taille réelle du stockage Amazon S3. Pour obtenir une estimation générale de la taille des données non compressées, vous pouvez multiplier par 10 la taille des journaux du compartiment S3. **Note** CloudTrail ne copiera pas un événement si sa durée est antérieure à la période de conservation spécifiée. Pour déterminer la période de conservation appropriée, faites la somme de l'événement le plus ancien que vous souhaitez copier en jours et du nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événement, comme le montre l'équation suivante : Durée de conservation = *oldest-event-in-days* + *number-days-to-retain*

Type de frais	Comment vous engagez les frais
	Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.
Conservation des données (données optimisées et compressées)	CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. La période de conservation d'un magasin de données d'événements détermine la durée pendant laquelle les données d'événements sont conservées dans le magasin de données d'événements. CloudTrail Lake détermine s'il convient de conserver un événement en vérifiant si la durée de l'événement se situe dans la période de conservation spécifiée. Par exemple, si vous spécifiez une période de conservation de 90 jours, les événements CloudTrail seront supprimés lorsque leur durée est supérieure à 90 jours. Pour les magasins de données d'événement utilisant l'option de tarification de rétention sur sept ans, le stockage est inclus dans le prix d'ingestion sans frais supplémentaires. Pour les magasins de données d'événement utilisant l'option de tarification de rétention extensible d'un an, le stockage est inclus gratuitement dans le prix d'ingestion pendant les 366 premiers jours (période de conservation par défaut). Après 366 jours, le stockage est proposé pay-as-you-pricing et facturé sur la base des données optimisées et compressées dans le magasin de données d'événements.

Type de frais	Comment vous engagez les frais
Exécution de requêtes dans CloudTrail Lake (données optimisées et compressées)	Lorsque vous exécutez des requêtes dans CloudTrail Lake, vous payez en fonction de la quantité de données optimisées et compressées numérisées.

Recommandations sur la manière de réduire les coûts

Cette section fournit des recommandations sur la manière de réduire les coûts lorsque vous travaillez avec CloudTrail Lake.

Choisissez une option de tarification en fonction du type d'événements que votre magasin de données d'événement collectera et de votre consommation mensuelle prévue

Lorsque vous créez un magasin de données d'événement, choisissez une option de tarification en fonction du type d'événements que votre magasin de données d'événement collectera et de votre consommation mensuelle prévue.

Si vous prévoyez d'ingérer moins de 25 To de données d'événements par mois et que vous souhaitez une période de conservation flexible allant jusqu'à 10 ans, choisissez l'option de tarification de rétention extensible d'un an. Nous recommandons également généralement cette option pour les magasins de données d'événements qui collectent des éléments de AWS Config configuration, des preuves d'Audit Manager et des événements provenant de l'extérieur AWS.

Si vous prévoyez d'ingérer plus de 25 To de données d'événements par mois et que vous avez besoin d'une période de conservation de 7 ans, choisissez l'option de tarification de rétention sur sept ans.

Évaluez l'ingestion mensuelle de votre magasin de données d'événement au fil du temps

Évaluez l'historique mensuel de l'ingestion de votre magasin de données d'événement pour voir s'il existe une option de tarification mieux adaptée à vos besoins.

Si vous possédez déjà un magasin de données d'événement qui utilise l'option de tarification de rétention sur sept ans et que vous ingérez moins de 25 To de données par mois, envisagez de mettre à jour le magasin de données d'événement pour utiliser un tarif de rétention extensible d'un an. Pour les magasins de données d'événements utilisant l'option de tarification de rétention sur sept ans, vous pouvez modifier l'option de tarification à l'aide de la CloudTrail console ou de UpdateEventDataStorel'API. AWS CLI

Si vous possédez déjà un magasin de données d'événement qui utilise l'option de tarification de rétention extensible d'un an et que vous ingérez plus de 25 To de données d'événement par mois, demandez-vous si la tarification de rétention sur sept ans ne serait pas mieux adaptée à vos besoins. Pour utiliser la nouvelle option de tarification, arrêtez l'ingestion sur votre magasin de données d'événement et créez un nouveau magasin de données d'événement avec l'option de tarification de rétention sur sept ans.

Utilisez des sélecteurs d'événements avancés pour filtrer les événements qui ne présentent aucun intérêt

Lorsque vous configurez un magasin de données d'événements pour CloudTrail la gestion ou les événements de données, filtrez les événements qui ne présentent aucun intérêt à l'aide de sélecteurs d'événements avancés.

Si vous créez un magasin de données d'événements pour collecter des événements de gestion, vous pouvez filtrer les événements de l'API de données Amazon Relational Database Service AWS Key Management Service (AWS KMS Amazon RDS) par filtrage (). Généralement, AWS KMS les actions telles que `EncryptDecrypt`, et `GenerateDataKey` génèrent plus de 99 % des événements.

Si vous créez un magasin de données d'événement pour collecter des données d'événement, vous pouvez utiliser des sélecteurs d'événements avancés pour filtrer les champs `eventName`, `resources.type`, `resources.ARN` et `readOnly`. Pour obtenir un exemple, consultez Exemple : création d'un magasin de données d'événements pour les événements de données S3.

Choisissez un intervalle de temps plus étroit lors de la copie des événements de journal de suivi

Lorsque vous copiez des événements de suivi vers CloudTrail Lake, spécifiez une heure de début et une heure de fin d'événement plus courtes afin de réduire la quantité de données ingérées.

Si vous copiez des événements de parcours dans CloudTrail Lake à des fins d'analyse historique et que vous ne souhaitez pas ingérer d'événements futurs, désélectionnez l'option d'ingestion d'événements afin de ne pas avoir à payer de frais pour l'ingestion d'événements supplémentaires.

Formater les requêtes pour utiliser un début et une fin **`eventTime`**

Lorsque vous exécutez des requêtes dans Lake, vous payez en fonction de la quantité de données analysées. Vous pouvez limiter les coûts en spécifiant le début et la fin `eventTime` de la requête.

Outils permettant de gérer les coûts

AWS Les budgets, une fonctionnalité de AWS Billing and Cost Management, vous permettent de définir des budgets personnalisés qui vous alertent lorsque vos coûts ou votre utilisation dépassent (ou devraient dépasser) le montant budgétisé.

Lorsque vous créez des banques de données sur les événements, la création d'un budget à l'aide de AWS budgets est une bonne pratique recommandée, qui peut vous aider à suivre vos CloudTrail dépenses. CloudTrail Les budgets basés sur les coûts aident à mieux faire connaître le montant qui pourrait vous être facturé pour votre CloudTrail utilisation. les alertes budgétaires vous avertissent lorsque votre facture atteint un seuil que vous définissez. Lorsque vous recevez une alerte de budget, vous pouvez effectuer des modifications avant la fin du cycle de facturation pour gérer vos coûts.

Après avoir créé un budget, vous pouvez l'utiliser AWS Cost Explorer pour voir comment vos CloudTrail coûts influencent votre AWS facture globale. Dans AWS Cost Explorer, après CloudTrail avoir ajouté le filtre Service, vous pouvez comparer vos CloudTrail dépenses historiques à celles de vos dépenses actuelles month-to-date (MTD), par région et par compte. Cette fonctionnalité vous permet de surveiller et de détecter les coûts imprévus dans vos CloudTrail dépenses mensuelles. Les fonctionnalités supplémentaires de Cost Explorer vous permettent de comparer les CloudTrail dépenses aux dépenses mensuelles au niveau des ressources spécifiques, en fournissant des informations sur les facteurs susceptibles d'entraîner des augmentations ou des baisses de coûts de votre facture.

Pour commencer à utiliser AWS les budgets, ouvrez AWS Billing and Cost Management, puis choisissez Budgets dans la barre de navigation de gauche. Nous vous recommandons de configurer des alertes budgétaires lorsque vous créez un budget afin de suivre CloudTrail les dépenses. Pour plus d'informations sur l'utilisation des AWS budgets, consultez les sections Gestion de vos coûts AWS Budgets et Bonnes pratiques en matière de AWS budgets.

Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake

Vous pouvez créer des balises de répartition des coûts définies par l'utilisateur pour suivre les coûts de requête et d'ingestion pour vos magasins de données d'événements CloudTrail Lake. Une balise de répartition des coûts définie par l'utilisateur est une paire clé-valeur que vous pouvez associer à un entrepôt de données d'événement. Après avoir activé les balises de répartition des coûts, AWS utilise les balises pour organiser les coûts des ressources dans votre rapport de répartition des coûts.

- Pour créer des balises dans la console, veuillez consulter l'étape 9 de la procédure Pour créer un magasin de données d'événements pour la CloudTrail gestion ou les événements de données.
- Pour créer des balises à l'aide de l' CloudTrail API, consultez CreateEventDataStoreet AddTagsdans le Guide de référence de l'AWS CloudTrail API.
- Pour créer des balises à l'aide de AWS CLI, voir create-event-data-storeet ajouter des balises dans le manuel de référence des AWS CLI commandes.

Pour plus d'informations sur l'activation des balises, veuillez consulter Activation des balises de répartition des coûts définies par l'utilisateur.

Consultez aussi

- Tarification AWS CloudTrail
- CloudWatch Métriques prises en charge
- Gérez vos coûts avec AWS Budgets
- Démarrage avec Cost Explorer

CloudWatch Métriques prises en charge

CloudTrail Lake prend en charge les CloudWatch métriques d'Amazon. CloudWatch est un service de surveillance des AWS ressources. Vous pouvez l'utiliser CloudWatch pour collecter et suivre les métriques, définir des alarmes et réagir automatiquement aux modifications de vos AWS ressources.

L'espace de `AWS/CloudTrail` noms inclut les métriques suivantes pour CloudTrail Lake.

Métrique	Description	Unités
`HourlyDataIngested`	La quantité de données ingérées dans l'entrepôt de données d'événements au cours de la dernière heure. Cette métrique est mise à jour toutes les heures. Cette métrique est disponibl e pour tous les types de	Octets

Métrique	Description	Unités
	magasins de données d’événement.	
`TotalDataRetained`	La quantité de données conservées dans l'entrepô t de données d'événements pendant toute sa période de conservation. Cette métrique est mise à jour toutes les nuits. Cette métrique est disponibl e pour tous les types de magasins de données d’événement.	Octets
`TotalStorageBytes`	Nombre total d’octets compressés dans le magasin de données d’événement au jour en cours. Cette métrique est disponibl e pour tous les types de magasins de données d’événement.	Octets

Métrique	Description	Unités
`TotalPaidStorageBytes`	Pour les magasins de données d'événements utilisant l'option de tarification de rétention extensible d'un an, il s'agit du nombre total d'octets compressés après 366 jours jusqu'à la période de rétention maximale configurée pour le magasin de données d'événement. Pour les magasins de données d'événement utilisant l'option de tarification de rétention extensible d'un an, le stockage est inclus sans frais supplémentaires avec le prix d'ingestion pendant les 366 premiers jours, qui est la période de conservation par défaut pour le magasin de données d'événement. Après 366 jours, le stockage est pay-as-you-go. Pour plus d'informations sur la tarification, consultez Tarification AWS CloudTrail. Cette mesure n'est disponible que pour les magasins de données d'événement utilisant l'option de tarification de rétention extensible d'un an.	Octets

Métrique	Description	Unités
`HourlyEventsAnalyzed`	Nombre total d'événements analysés par CloudTrail Insights dans le magasin de données d'événements. Cette métrique est mise à jour toutes les heures. Cette métrique concerne les magasins de données d'événements CloudTrail qui activent CloudTrail Insights.	Nombre

Pour plus d'informations sur CloudWatch les métriques, consultez les rubriques suivantes.

- Utilisation des CloudWatch métriques Amazon
- Utilisation des CloudWatch alarmes Amazon

Travailler avec les CloudTrail sentiers

Les sentiers enregistrent les AWS activités, diffusent et stockent ces événements dans un compartiment Amazon S3, avec une livraison facultative à CloudWatch Logs et Amazon EventBridge.

Vous pouvez envoyer une copie de vos événements de gestion en cours à votre compartiment S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

Vous pouvez créer deux types de sentiers pour un Compte AWS : les sentiers multirégionaux et les sentiers à région unique.

Sentiers multirégionaux

Lorsque vous créez un journal multirégional, enregistrez CloudTrail les événements dans l'ensemble Régions AWS de la AWS partition sur laquelle vous travaillez et délivre les fichiers journaux d' CloudTrail événements dans un compartiment S3 que vous spécifiez. Si un Région AWS est ajouté après avoir créé un parcours multirégional, cette nouvelle région est automatiquement incluse et les événements de cette région sont enregistrés. La création d'un journal de suivi multi-régions est une bonne pratique recommandée, car vous pouvez journaliser l'activité dans toutes les régions dans votre compte. Tous les sentiers que vous créez à l'aide de la CloudTrail console sont multirégionaux. Vous pouvez convertir un parcours à région unique en un parcours multirégional à l'aide du. AWS CLI Pour plus d'informations, consultez Créer un journal de suivi dans la console et Convertir un journal de suivi qui s'applique à une région de sorte qu'il s'applique à toutes les régions.

Sentiers d'une seule région

Lorsque vous créez un parcours d'une seule région, CloudTrail enregistre les événements de cette région uniquement. Il fournit ensuite les fichiers journaux d' CloudTrail événements à un compartiment Amazon S3 que vous spécifiez. Vous ne pouvez créer un journal de suivi à région unique qu'à l'aide de l' AWS CLI. Si vous créez des pistes uniques supplémentaires, vous pouvez faire en sorte que ces pistes fournissent des fichiers journaux d' CloudTrail événements dans le même compartiment S3 ou dans des compartiments séparés. Il s'agit de l'option par défaut lorsque vous créez un parcours à l'aide de l'API AWS CLI ou de l' CloudTrail API. Pour plus d'informations, consultez Création, mise à jour et gestion de sentiers à l'aide du AWS CLI.

> **Note**
>
> Pour les deux types de journaux de suivi, vous pouvez spécifier un compartiment Amazon S3 de n'importe quelle région.

Si vous avez créé une organisation dans AWS Organizations, vous pouvez créer un journal d'organisation qui enregistre tous les événements pour tous les AWS comptes de cette organisation. Les parcours d'organisation peuvent s'appliquer à toutes les AWS régions ou à la région actuelle. Les journaux de suivi d'une organisation doivent être créés en utilisant le compte de gestion et, s'il est spécifié qu'ils s'appliquent à une organisation, ils sont automatiquement appliqués à tous les comptes membres de l'organisation. Les comptes membres peuvent consulter l'historique de l'organisation, mais ne peuvent ni le modifier ni le supprimer. Par défaut, les comptes membres n'ont pas accès aux fichiers journaux d'un journal de suivi d'organisation dans le compartiment Amazon S3. Pour plus d'informations, voir Création d'un journal de suivi pour une organisation.

Rubriques

Création d'un parcours pour votre Compte AWS

Lorsque vous créez un journal de suivi, vous activez la livraison continue d'événements en tant que fichiers journaux à un compartiment Amazon S3 que vous spécifiez. La création d'un journal de suivi présente de nombreux bénéfices, notamment:

- Un registre d'événements qui s'étend au-delà des 90 derniers jours.

- La possibilité de surveiller et d'alerter automatiquement en cas d'événements spécifiques en envoyant des événements de journal à Amazon CloudWatch Logs.
- Possibilité d'interroger les journaux et d'analyser l'activité des AWS services avec Amazon Athena.

À compter du 12 avril 2019, vous ne pourrez consulter les sentiers que dans les AWS régions où ils enregistrent des événements. Si vous créez un journal qui enregistre les événements dans toutes les AWS régions, il apparaît dans la console dans toutes les régions de la AWS partition dans laquelle vous travaillez. Si vous créez un journal de suivi qui enregistre des événements dans une seule région , vous pouvez l'afficher et le gérer uniquement dans cette région . La création d'un parcours multirégional est l'option par défaut si vous créez un parcours à l'aide de la AWS CloudTrail console. Il s'agit d'une bonne pratique recommandée. Pour créer un journal de suivi pour une seule région, il convient d'utiliser l' AWS CLI.

Si vous l'utilisez AWS Organizations, vous pouvez créer un journal qui enregistrera les événements de tous les AWS comptes de l'organisation. Un journal de suivi avec le même nom sera créé dans chaque compte membre, et les événements de chaque journal de suivi seront envoyés au compartiment Amazon S3 que vous spécifiez.

> **Note**
>
> Seuls les comptes de gestion ou d'administrateur délégué d'une organisation peut créer un journal de suivi pour cette organisation. La création d'un parcours pour une organisation permet automatiquement l'intégration entre CloudTrail et Organizations. Pour plus d'informations, voir Création d'un journal de suivi pour une organisation.

Rubriques

- Création et mise à jour d'un journal d'activité à l'aide de la console
- Création, mise à jour et gestion de sentiers à l'aide du AWS CLI

Création et mise à jour d'un journal d'activité à l'aide de la console

Vous pouvez utiliser la CloudTrail console pour créer, mettre à jour ou supprimer vos parcours. Les journaux de suivi créés à l'aide de la console sont multi-régions. Pour créer un journal qui enregistre les événements dans un seul fichier Région AWS, utilisez le AWS CLI.

Vous pouvez créer jusqu'à cinq journaux de suivi pour chaque région. Après avoir créé un suivi, commence CloudTrail automatiquement à consigner les appels d'API et les événements associés dans votre compte dans le compartiment Amazon S3 que vous spécifiez. Pour arrêter la journalisation, il est possible de désactiver la journalisation pour le journal d'activité ou supprimer ce dernier.

L'utilisation de la CloudTrail console pour créer ou mettre à jour un journal présente les avantages suivants.

- Si c'est la première fois que vous créez un parcours, la CloudTrail console vous permet de visualiser les fonctionnalités et options disponibles.
- Si vous configurez un journal pour consigner les événements liés aux données, la CloudTrail console vous permet de visualiser les types de données disponibles. Pour plus d'informations sur la journalisation des événements de données, veuillez consulter Journalisation des événements de données.

Pour obtenir des informations spécifiques à la création d'un suivi pour une organisation dans AWS Organizations, voirCréation d'un journal de suivi pour une organisation.

Rubriques

- Création d'un journal de suivi
- Mise à jour d'un journal de suivi
- Suppression d'un journal de suivi
- Désactivation de la journalisation pour un journal d'activité

Création d'un journal de suivi

En guise de bonnes pratiques, créez un journal de suivi qui s'applique à toutes les Régions AWS. Il s'agit du paramètre par défaut lorsque vous créez un parcours dans la CloudTrail console. Lorsqu'un suivi s'applique à toutes les régions, CloudTrail envoie les fichiers journaux de toutes les régions de la AWS partition dans laquelle vous travaillez vers un compartiment S3 que vous spécifiez. Après avoir créé le parcours, commence AWS CloudTrail automatiquement à enregistrer les événements que vous avez spécifiés.

> **Note**
>
> Après avoir créé un suivi, vous pouvez en configurer un autre Services AWS pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez AWS intégrations de services avec journaux CloudTrail .

Rubriques

- Créer un journal de suivi dans la console
- Étapes suivantes

Créer un journal de suivi dans la console

Utilisez la procédure suivante pour créer un journal qui enregistre les événements dans l'ensemble Régions AWS de la AWS partition sur laquelle vous travaillez. Il s'agit d'une bonne pratique recommandée. Pour journaliser les événements dans une région unique (non recommandé), utilisez l' AWS CLI.

Pour créer un CloudTrail parcours à l'aide du AWS Management Console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Sur la page d'accueil du CloudTrail service, sur la page des sentiers ou dans la section des sentiers de la page du tableau de bord, choisissez Créer un parcours.
3. Sur la page Créer un journal de suivi, tapez un nom pour votre journal de suivi dans la zone Nom du journal de suivi. Pour plus d'informations, consultez Exigences de dénomination.
4. S'il s'agit d'un suivi d' AWS Organizations organisation, vous pouvez activer le suivi pour tous les comptes de votre organisation. Pour voir cette option, vous devez vous connecter à la console avec un utilisateur ou un rôle dans le compte de gestion ou d'administrateur délégué. Pour créer avec succès le journal de suivi d'une organisation, assurez-vous que l'utilisateur ou le rôle dispose d'autorisations suffisantes. Pour plus d'informations, consultez Création d'un journal de suivi pour une organisation.
5. Sous Emplacement de stockage, choisissez Créer un nouveau compartiment S3 pour créer un nouveau compartiment. Lorsque vous créez un bucket, il CloudTrail crée et applique les politiques de bucket requises. Si vous choisissez de créer un nouveau compartiment S3, votre

politique IAM doit inclure une autorisation pour l'`s3:PutEncryptionConfiguration`action, car le chiffrement côté serveur est activé par défaut pour le compartiment.

> **Note**
>
> Si vous avez choisi Utiliser un compartiment S3 existant, spécifiez un compartiment dans Nom du compartiment des journaux de suivi, ou sélectionnez Parcourir pour choisir un compartiment. Si vous voulez utiliser un compartiment dans un autre compte, vous devez spécifier le nom du compartiment. La politique du compartiment doit accorder CloudTrail l'autorisation d'y écrire. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.

Pour retrouver plus facilement vos journaux, créez un nouveau dossier (également appelé préfixe) dans un compartiment existant pour stocker vos CloudTrail journaux. Saisir le préfixe dans Préfixe.

6. Sous Chiffrement SSE-KMS du fichier journal, choisissez Activé si vous souhaitez chiffrer vos fichiers journaux avec SSE-KMS plutôt qu'avec SSE-S3. La valeur par défaut est Activé. Si vous n'activez pas le chiffrement SSE-KMS, vos journaux sont chiffrés à l'aide du chiffrement SSE-S3. Pour plus d'informations sur le chiffrement SSE-KMS, voir Utilisation du chiffrement côté serveur avec AWS Key Management Service (SSE-KMS). Pour plus d'informations sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3).

   Si vous activez le chiffrement SSE-KMS, sélectionnez Nouveau ou Existant. AWS KMS key Dans AWS KMS Alias, spécifiez un alias au format `alias/` *`MyAliasName`*. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

   > **Note**
   >
   > Vous pouvez également saisir l'ARN d'une clé à partir d'un autre compte. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS. La politique de clé doit CloudTrail autoriser l'utilisation de la clé pour chiffrer vos fichiers

journaux et permettre aux utilisateurs que vous spécifiez de lire les fichiers journaux sous forme non chiffrée. Pour en savoir plus sur la modification manuelle de la politique de clés, consultez Configurer les politiques AWS KMS clés pour CloudTrail.

7. Sous Paramètres supplémentaires, configurez les événements suivants.

   a. Sous Validation du fichier journal, choisissez Activé pour que les fichiers de valeur de hachage soient livrés dans votre compartiment S3. Vous pouvez utiliser les fichiers de synthèse pour vérifier que vos fichiers journaux n'ont pas changé après leur CloudTrail livraison. Pour plus d'informations, consultez Validation de l' CloudTrail intégrité du fichier journal.

   b. Pour l'envoi de notifications SNS, choisissez Enabled pour être averti chaque fois qu'un journal est envoyé à votre bucket. CloudTrail enregistre plusieurs événements dans un fichier journal. Des notifications SNS sont envoyées pour chaque fichier journal, non pour chaque événement. Pour plus d'informations, consultez Configuration des notifications Amazon SNS pour CloudTrail.

      Si vous activez les notifications SNS, pour Créer une nouvelle rubrique SNS, choisissez Nouveau pour créer une rubrique, ou Existant, pour utiliser une rubrique existante. Si vous créez un journal de suivi qui s'applique à toutes les régions, les notifications SNS relatives à la livraison de fichiers journaux de toutes les régions sont envoyées à la rubrique SNS unique que vous créez.

      Si vous choisissez Nouveau, vous CloudTrail spécifiez un nom pour le nouveau sujet ou vous pouvez saisir un nom. Si vous choisissez Existant, choisissez une rubrique SNS dans la liste déroulante. Vous pouvez également saisir l'ARN d'une rubrique provenant d'une autre région ou d'un compte disposant des autorisations appropriées. Pour plus d'informations, consultez Politique relative aux rubriques Amazon SNS pour CloudTrail.

      Si vous créez une rubrique, vous devez vous abonner à la rubrique pour être averti de l'envoi de fichiers journaux. Vous pouvez vous abonner à partir de la console Amazon SNS. En raison de la fréquence des notifications, nous vous recommandons de configurer l'abonnement pour pouvoir utiliser une file d'attente Amazon SQS afin de gérer les notifications par programmation. Pour plus d'informations, consultez Prise en main d'Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

8. Vous pouvez éventuellement configurer CloudTrail pour envoyer des fichiers CloudWatch journaux à Logs en choisissant Enabled in CloudWatch Logs. Pour plus d'informations, consultez Envoyer des événements à CloudWatch Logs.

   a. Si vous activez l'intégration aux CloudWatch journaux, choisissez Nouveau pour créer un nouveau groupe de journaux ou Existant pour utiliser un groupe existant. Si vous choisissez Nouveau, vous CloudTrail spécifiez un nom pour le nouveau groupe de journaux ou vous pouvez saisir un nom.

   b. Si vous choisissez Existant, choisissez un groupe de journaux dans la liste déroulante.

   c. Choisissez Nouveau pour créer un nouveau rôle IAM afin d'obtenir les autorisations d'envoyer des CloudWatch journaux à Logs. Choisir Existant pour choisir un rôle IAM existant dans la liste déroulante. L'instruction de politique pour le rôle nouveau ou existant s'affiche lorsque vous déroulez Document de politique. Pour plus d'informations sur ce rôle, consultez Document de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance.

   > **Note**
   >
   > - Lorsque vous configurez un journal de suivi, vous pouvez choisir un compartiment S3 et une rubrique SNS qui appartiennent à un autre compte. Toutefois, si vous souhaitez CloudTrail transmettre des événements à un groupe de CloudWatch journaux journaux, vous devez choisir un groupe de journaux existant dans votre compte actuel.
   > - Seul le compte de gestion peut configurer un groupe de CloudWatch journaux pour un journal d'entreprise à l'aide de la console. L'administrateur délégué peut configurer un groupe de CloudWatch journaux Logs à l'aide des opérations AWS CLI CloudTrail `CreateTrail` ou de `UpdateTrail` l'API.

9. Pour Balises, ajoutez une ou plusieurs identifications personnalisées (paires clé-valeur) à votre journal de suivi. Les balises peuvent vous aider à identifier à la fois vos CloudTrail traces et les compartiments Amazon S3 contenant les fichiers CloudTrail journaux. Vous pouvez ensuite utiliser des groupes de ressources pour vos CloudTrail ressources. Pour plus d'informations, consultez AWS Resource Groups et Balises.

10. Sur la page Choisir des événements du journal, choisissez les types d'événements que vous souhaitez consigner. Sous Événements de gestion, procédez comme suit.

a. Pour Activité d'API, indiquez si vous souhaitez que votre journal de suivi journalise les événements en événements Lecture ou en événements Écriture, ou les deux. Pour plus d'informations, consultez Événements de gestion.

b. Choisissez Exclure les AWS KMS événements pour filtrer AWS Key Management Service (AWS KMS) les événements de votre parcours. Le paramètre par défaut est d'inclure tous les AWS KMS événements.

   L'option permettant d'enregistrer ou d'exclure AWS KMS des événements n'est disponible que si vous enregistrez des événements de gestion sur votre parcours. Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

   AWS KMS des actions telles que `Encrypt`Decrypt, et génèrent `GenerateDataKey` généralement un grand volume (plus de 99 %) d'événements. Ces actions sont désormais journalisées en tant qu'événements Lecture. Les AWS KMS actions pertinentes à faible volume telles que `DisableDelete`, et `ScheduleKey` (qui représentent généralement moins de 0,5 % du volume d' AWS KMS événements) sont enregistrées en tant qu'événements d'écriture.

   Pour exclure des événements importants tels que`Encrypt`, et `DecryptGenerateDataKey`, tout en enregistrant les événements pertinents tels que`Disable`, `Delete` et`ScheduleKey`, choisissez de consigner les événements de gestion d'écriture et décochez la case Exclure les AWS KMS événements.

c. Choisissez Exclure les événements API de données Amazon RDS pour filtrer les événements d'API de données Amazon Relational Database Service Data hors de votre journal de suivi. Le paramètre par défaut consiste à inclure tous les événements d'API de données Amazon RDS. Pour plus d'informations sur les événements d'API Amazon RDS Data API, consultez Journalisation des appels d'API de données avec AWS CloudTrail dans le Guide de l'utilisateur Amazon RDS pour Aurora.

11. Pour journaliser les événements de données, choisissez Événements de données. Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour plus d'informations, consultez Tarification AWS CloudTrail.

12. **Important**

    Les étapes 12 à 16 concernent la configuration des événements de données à l'aide de sélecteurs d'événements avancés, ce qui est le cas par défaut. Les sélecteurs d'événements avancés vous permettent de configurer davantage de types d'événements de données et de contrôler avec précision les événements de données capturés par votre journal de suivi. Si vous avez choisi d'utiliser des sélecteurs d'événements de base, suivez les étapes décrites dans Configurer les paramètres des événements de données à l'aide de sélecteurs d'événements de base, puis revenez à l'étape 17 de cette procédure.

    Pour Type d'événement de données, choisissez le type de ressource sur lequel vous souhaitez journaliser les événements de données. Pour plus d'informations sur les types d'événements de données, veuillez consulter Événements de données.

    Note

    Pour enregistrer les événements de données pour AWS Glue les tables créées par Lake Formation, choisissez Lake Formation.

13. Choisissez un modèle de sélecteur de journaux. CloudTrail inclut des modèles prédéfinis qui enregistrent tous les événements de données pour le type de ressource. Pour créer un modèle de sélecteur de journal personnalisé, choisissez Personnaliser.

    Note

    Le choix d'un modèle prédéfini pour les compartiments S3 permet de consigner les événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois le suivi terminé.
    Il permet également de consigner l'activité des événements de données effectuée par n'importe quelle identité IAM de votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
    Si le journal de suivi s'applique à une seule région, le fait de choisir un modèle prédéfini qui journalise tous les compartiments S3 permet la journalisation des événements de données pour tous les compartiments situés dans la même région que votre journal de suivi et tous les compartiments que vous créerez ultérieurement dans cette région. Les

événements de données relatifs aux compartiments Amazon S3 situés dans d'autres régions ne seront pas enregistrés dans votre AWS compte.
Si vous créez un suivi pour toutes les régions, le choix d'un modèle prédéfini pour les fonctions Lambda permet d'enregistrer les événements de données pour toutes les fonctions actuellement présentes dans votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans n'importe quelle région une fois le suivi créé. Si vous créez un suivi pour une seule région (en utilisant le AWS CLI), cette sélection active l'enregistrement des événements de données pour toutes les fonctions actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une fois que vous aurez fini de créer le journal. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions.
La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectuée par n'importe quelle identité IAM de votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

14. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.
15. Dans Sélecteurs d'événements avancés, créez une expression pour les ressources spécifiques sur lesquelles vous souhaitez journaliser les événements de données. Vous pouvez ignorer cette étape si vous utilisez un modèle de journal prédéfini.

    a. Choisissez parmi les options suivantes.

    - **`readOnly`**- `readOnly` peut être défini pour être égal à une valeur de `true` ou`false`. Les événements de données en lecture seule sont des événements qui ne modifient pas l'état d'une ressource, tels que les événements `Get*` ou `Describe*`. Les événements d'écriture ajoutent, modifient ou suppriment des ressources, des attributs ou des artefacts, tels que les événements `Put*`, `Delete*`, ou `Write*`. Pour journaliser les deux événements `read` et `write`, n'ajoutez pas de sélecteur `readOnly`.
    - **`eventName`** - `eventName` peut utiliser n'importe quel opérateur. Vous pouvez l'utiliser pour inclure ou exclure tout événement de données enregistré CloudTrail, tel que `PutBucketPutItem`, ou`GetSnapshotBlock`.

- **`resources.ARN`**- Vous pouvez utiliser n'importe quel opérateur`resources.`ARN, mais si vous utilisez égal ou non, la valeur doit correspondre exactement à l'ARN d'une ressource valide du type que vous avez spécifié dans le modèle comme valeur de`resources.type`.

  Le tableau suivant affiche le format ARN valide de chaque `resources.type`.

  > **Note**
  >
  > Vous ne pouvez pas utiliser le `resources.`ARN champ pour filtrer les types de ressources dépourvus d'ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	resources.ARN
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
`AWS::Timestream::Database`	`arn:partition :timestre am: region:account_ID :database / database_name`
`AWS::Timestream::Table`	`arn:partition :timestre am: region:account_ID :database / database_name /table/table_name`
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Pour les tables ayant les flux activés, le champ `resources` dans l'événement de plan de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.

[2] Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante. La barre oblique de fin est intentionnelle ; ne l'excluez pas.

[3] Pour journaliser les événements sur tous les objets d'un point d'accès S3, il est recommandé d'utiliser uniquement l'ARN du point d'accès, de ne pas inclure le chemin d'accès de l'objet et d'utiliser les opérateurs `StartsWith` ou `NotStartsWith`.

Pour plus d'informations sur les formats ARN des ressources d'événements de données, consultez Actions, ressources et clés de condition dans le Guide de l'utilisateur AWS Identity and Access Management .

b. Pour chaque champ, choisissez + Conditions pour ajouter autant de conditions que vous le souhaitez, jusqu'à un maximum de 500 valeurs spécifiées pour toutes les conditions. Par exemple, pour exclure les événements de données de deux compartiments S3 des

événements de données enregistrés sur votre parcours, vous pouvez définir le champ sur Resources.ARN, définir l'opérateur pour ne commence pas par, puis coller l'ARN d'un compartiment S3 ou rechercher les compartiments S3 pour lesquels vous ne souhaitez pas enregistrer d'événements.

Pour ajouter le deuxième compartiment S3, choisissez + Conditions, puis répétez l'instruction précédente, en collant dans l'ARN ou en recherchant un compartiment différent.

> **Note**
>
> Il est possible de définir un maximum de 500 valeurs pour tous les sélecteurs d'un journal de suivi. Cela inclut des tableaux de valeurs multiples pour un sélecteur tel que `eventName`. Si vous avez défini des valeurs uniques pour tous les sélecteurs, il est possible d'ajouter un maximum de 500 conditions à un sélecteur.
> Si votre compte compte compte plus de 15 000 fonctions Lambda, vous ne pouvez pas afficher ou sélectionner toutes les fonctions dans la CloudTrail console lors de la création d'un journal. Il est toujours possible de journaliser toutes les fonctions à l'aide d'un modèle de sélecteur prédéfini, même si ces dernières ne sont pas affichées. Si vous souhaitez journaliser les événements de données de fonctions spécifiques, vous pouvez ajouter manuellement une fonction si vous connaissez son ARN. Vous pouvez également terminer la création du journal dans la console, puis utiliser la put-event-selectors commande AWS CLI et pour configurer la journalisation des événements de données pour des fonctions Lambda spécifiques. Pour plus d'informations, consultez Gérer les sentiers à l'aide du AWS CLI.

c. Choisir + champ pour ajouter des champs supplémentaires au besoin. Pour éviter les erreurs, il convient de ne pas définir de valeurs conflictuelles ou en double pour les champs. Par exemple, ne spécifiez pas un ARN dans un sélecteur pour être égal à une valeur, puis spécifiez que l'ARN n'est pas égal à la même valeur dans un autre sélecteur.

16. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Ajouter un type d'événement de données. Répétez les étapes 12 à cette étape pour configurer les sélecteurs d'événements avancés pour le type d'événement de données.
17. Choisissez Insights events si vous souhaitez que votre parcours enregistre les événements CloudTrail Insights.

    Dans Type d'événement, sélectionnez Événements Insights. Vous devez journaliser les événements de gestion Écriture pour journaliser les événements Insights afin de connaître le

Taux d'appels d'API. Vous devez journaliser les événements de gestion Lecture ou Écriture pour journaliser les événements Insights afin de connaître le Taux d'erreur de l'API.

CloudTrail Insights analyse les événements de gestion pour détecter toute activité inhabituelle et enregistre les événements lorsque des anomalies sont détectées. Par défaut, les journaux de suivi ne journalisent pas les événements Insights. Pour plus d'informations sur les événements Insights, consultez Journalisation des événements Insights. Des frais supplémentaires s'appliquent pour la journalisation des événements Insights. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

Les événements Insights sont transmis à un dossier différent nommé `/CloudTrail-Insight` dans le même compartiment S3 spécifié dans la zone Emplacement de stockage de la page de détails du journal. CloudTrailcrée le nouveau préfixe pour vous. Par exemple, si votre compartiment S3 de destination actuel se nomme `S3bucketName/AWSLogs/CloudTrail/`, le nom du compartiment S3 avec un nouveau préfixe se nommera `S3bucketName/AWSLogs/CloudTrail-Insight/`.

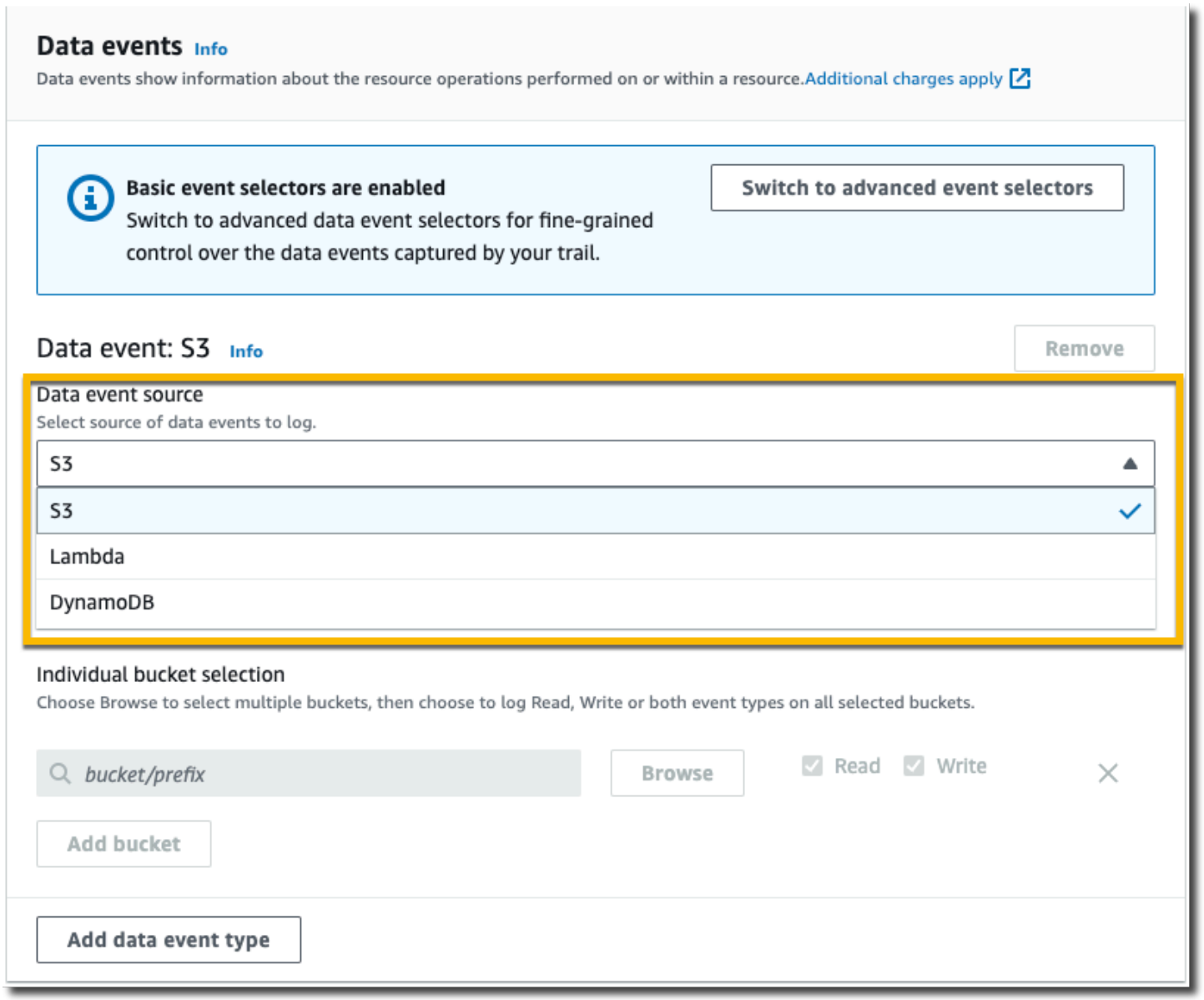
18. Après avoir sélectionné les types d'événements à journaliser, choisissez Suivant.
19. Sur la page Vérifier et créer, vérifiez vos choix. Choisissez Modifier dans une section pour modifier les paramètres de journal de suivi affichés dans cette section. Lorsque vous êtes prêt à créer votre journal de suivi, choisissez Créer un journal de suivi.
20. Le nouveau journal de suivi s'affiche sur la page Journaux de suivi. En 5 minutes environ, CloudTrail publie des fichiers journaux qui indiquent les appels AWS d'API effectués dans votre compte. Les fichiers journaux se trouvent dans le compartiment S3 que vous avez spécifié. Le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 36 heures si vous avez activé la journalisation des événements Insights et qu'une activité inhabituelle est détectée.

> **Note**
>
> CloudTrail fournit généralement des journaux dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti. Pour plus d'informations, consultez le Contrat de niveau de service (SLA)AWS CloudTrail.
> Si vous configurez mal votre trace (par exemple, si le compartiment S3 est inaccessible), vous CloudTrail tenterez de remettre les fichiers journaux à votre compartiment S3 pendant 30 jours, et ces attempted-to-deliver événements seront soumis aux frais standard. CloudTrail Pour éviter des frais sur un journal de suivi mal configuré, vous devez supprimer le journal de suivi.

Configurer les paramètres des événements de données à l'aide de sélecteurs d'événements de base

Vous pouvez utiliser des sélecteurs d'événements avancés pour configurer tous les types d'événements de données. Les sélecteurs d'événements avancés vous permettent de créer des sélecteurs précis pour enregistrer uniquement les événements qui vous intéressent.

Si vous utilisez des sélecteurs d'événements de base pour enregistrer des événements de données, vous êtes limité à la journalisation des événements de données pour les compartiments, les AWS Lambda fonctions et les tables Amazon DynamoDB d'Amazon S3. Vous ne pouvez pas filtrer sur le `eventName` terrain à l'aide de sélecteurs d'événements de base.



Utilisez la procédure suivante afin de configurer les paramètres des événements de données à l'aide de sélecteurs d'événements de base.

Pour configurer les paramètres des événements de données à l'aide de sélecteurs d'événements de base

1. Dans Événements, sélectionnez Événements de données pour journaliser les événements de données. Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour plus d'informations, consultez Tarification AWS CloudTrail.
2. Pour les compartiments Amazon S3 :

   a. Pour Data event source (Source d'événements de données), choisissez S3.

   b. Il est possible de choisir de journaliser Tous les compartiments S3 actuels et futurs ou de spécifier des compartiments ou fonctions individuels. Par défaut, les événements de données sont journalisés pour tous les compartiments S3 actuels et futurs.

      > **Note**
      >
      > Le maintien de l'option par défaut Tous les compartiments S3 actuels et futurs active la journalisation des événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois le suivi terminé. Il permet également de consigner l'activité des événements de données effectuée par n'importe quelle identité IAM de votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
      > Si vous créez un parcours pour une seule région (à l'aide du AWS CLI), sélectionnez Tous les compartiments S3 actuels et futurs pour enregistrer les événements de données pour tous les compartiments de la même région que votre parcours et pour tous les compartiments que vous créerez ultérieurement dans cette région. Les événements de données relatifs aux compartiments Amazon S3 situés dans d'autres régions ne seront pas enregistrés dans votre AWS compte.

   c. Si vous laissez l'option par défaut, Tous les compartiments S3 actuels et futurs, choisissez de journaliser les événements de lecture, les événements d'écriture, ou les deux.

   d. Pour sélectionner des compartiments individuels, il convient de vider les boîtes de dialogue Lecture et Écriture pour Tous les compartiments S3 actuels et futurs. Dans Sélection du compartiment individuel, recherchez un compartiment sur lequel journaliser

les événements de données. Recherchez des compartiments spécifiques en tapant un préfixe de compartiment pour le compartiment souhaité. Vous pouvez sélectionner plusieurs compartiments dans cette fenêtre. Choisissez Ajouter un compartiment pour journaliser les événements de données pour d'autres compartiments. Choisissez de journaliser les événements Lecture tels que `GetObject`, les événements Écriture tels que `PutObject`, ou les deux.

Ce paramètre est prioritaire par rapport aux paramètres que vous définissez pour les compartiments individuels. Par exemple, si vous spécifiez la journalisation des événements Read (Lecture) pour tous les compartiments S3, puis choisissez d'ajouter un compartiment spécifique pour la journalisation des événements de données, Read (Lecture) est déjà sélectionné pour le compartiment que vous avez ajouté. Vous ne pouvez pas effacer la sélection. Vous pouvez uniquement configurer l'option pour Écriture.

Pour supprimer un compartiment de la journalisation, choisissez X.

3. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données).
4. Pour les fonctions Lambda :

   a. Pour Data event source (Source d'événement de données), choisissez Lambda.

   b. Dans Fonction Lambda, choisissez Toutes les régions pour journaliser toutes les fonctions Lambda, ou Fonction d'entrée en tant qu'ARN, pour consigner les événements de données sur une fonction spécifique.

   Pour enregistrer les événements de données relatifs à toutes les fonctions Lambda de votre AWS compte, sélectionnez Enregistrer toutes les fonctions actuelles et futures. Ce paramètre est prioritaire par rapport aux paramètres que vous définissez pour les fonctions individuelles. Toutes les fonctions sont journalisées, même si elles ne sont pas toutes affichées.

   > **Note**
   >
   > Si vous créez un journal de suivi pour toutes les régions, cette sélection active la journalisation des événements de données pour toutes les fonctions se trouvant actuellement dans votre compte AWS et pour toute fonction Lambda que vous êtes susceptible de définir dans n'importe quelle région après avoir achevé la création du journal de suivi. Si vous créez un suivi pour une seule région (en utilisant le AWS CLI), cette sélection active l'enregistrement des événements de données pour toutes

les fonctions actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une fois que vous aurez fini de créer le journal. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions. La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectuée par n'importe quelle identité IAM de votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

c. Si vous choisissez Fonction d'entrée en tant qu'ARN, saisissez l'ARN d'une fonction Lambda.

> **Note**
>
> Si votre compte compte compte plus de 15 000 fonctions Lambda, vous ne pouvez pas afficher ou sélectionner toutes les fonctions dans la CloudTrail console lors de la création d'un journal. Vous pouvez toujours sélectionner l'option de journalisation de toutes les fonctions, même si elles ne sont pas affichées. Si vous souhaitez journaliser les événements de données de fonctions spécifiques, vous pouvez ajouter manuellement une fonction si vous connaissez son ARN. Vous pouvez également terminer la création du journal dans la console, puis utiliser la put-event-selectors commande AWS CLI et pour configurer la journalisation des événements de données pour des fonctions Lambda spécifiques. Pour plus d'informations, consultez Gérer les sentiers à l'aide du AWS CLI.

5. Pour Tables DynamoDB :

   a. Pour Data event source (Source d'événement de données), choisissez DynamoDB.

   b. Dans Sélection d'une table DynamoDB, choisissez Parcourir pour sélectionner une table ou coller dans l'ARN d'une table DynamoDB à laquelle vous avez accès. Un ARN de table DynamoDB utilise le format suivant :

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   Pour ajouter une autre table, choisissez Ajouter une ligne, puis recherchez un tableau ou collez dans l'ARN d'une table à laquelle vous avez accès.

6. Pour configurer les événements Insights et d'autres paramètres pour votre piste, revenez à la procédure précédente dans cette rubrique, ???.

Étapes suivantes

Après avoir créé le journal de suivi, vous pouvez le modifier:

- Si ce n'est pas déjà fait, vous pouvez configurer CloudTrail pour envoyer des fichiers CloudWatch journaux à Logs. Pour plus d'informations, consultez Envoyer des événements à CloudWatch Logs.
- Créez une table et utilisez-la pour exécuter une requête dans Amazon Athena afin d'analyser l'activité de vos services AWS . Pour plus d'informations, consultez la section Création d'une table pour les CloudTrail journaux dans la CloudTrail console dans le guide de l'utilisateur d'Amazon Athena.
- Ajoutez des identifications personnalisées (paires clé-valeur) pour le journal de suivi.
- Pour créer un autre journal de suivi, ouvrez la page Journaux de suivi et choisissez Créer un journal de suivi.

Mise à jour d'un journal de suivi

Cette section décrit comment modifier les paramètres du journal de suivi.

Pour mettre à jour un suivi régional afin de consigner les événements dans l'ensemble Régions AWS de la AWS partition dans laquelle vous travaillez, ou pour mettre à jour un journal multirégional pour n'enregistrer les événements que dans une seule région, vous devez utiliser le. AWS CLI Pour plus d'informations sur la mise à jour d'un journal de suivi à région unique pour journaliser les événements dans toutes les régions, veuillez consulter Convertir un journal de suivi qui s'applique à une région de sorte qu'il s'applique à toutes les régions. Pour plus d'informations sur la mise à jour d'un journal de suivi multi-régions pour journaliser les événements dans une région unique, veuillez consulter Convertir un journal de suivi multi-régions à un journal de suivi à région unique.

Si vous avez activé les événements CloudTrail de gestion dans Amazon Security Lake, vous devez gérer au moins un journal organisationnel multirégional qui enregistre à la fois les `read` événements de gestion et les événements `write` de gestion. Vous ne pouvez pas mettre à jour un journal de suivi éligible de telle sorte qu'il ne réponde pas aux exigences de Security Lake. Par exemple, en modifiant le journal de suivi pour qu'il s'applique à une région unique ou en désactivant la journalisation des événements de gestion `read` et `write`.

> **Note**
>
> CloudTrail met à jour les traces de l'organisation dans les comptes des membres même en cas d'échec de la validation des ressources. Voici des exemples d'échecs de validation :
>
> - une politique de compartiment Amazon S3 incorrecte
> - une politique de rubrique Amazon SNS incorrecte
> - impossibilité de livrer à un groupe de CloudWatch journaux Logs
> - autorisation insuffisante pour chiffrer à l'aide d'une clé KMS
>
> Un compte membre disposant d' CloudTrail autorisations peut voir les échecs de validation d'un journal d'organisation en consultant la page de détails du journal sur la CloudTrail console ou en exécutant la AWS CLI get-trail-statuscommande.

Pour mettre à jour un parcours à l'aide du AWS Management Console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation de gauche, choisissez Trails (Journaux de suivi), puis le nom du journal de suivi.
3. Dans Renseignements généraux, choisissez Modifier pour modifier les paramètres suivants. Vous ne pouvez pas modifier le nom d'un journal de suivi.

   - Appliquer le parcours à mon organisation - Indiquez si ce parcours est un parcours d' AWS Organizations organisation.

     > **Note**
     >
     > Seul le compte de gestion de l'organisation peut convertir un journal de suivi organisationnel en journal de suivi non lié à une organisation, ou effectuer la conversion inverse.

   - Emplacement de journalisation du journal de suivi : modifiez le nom du compartiment S3 ou du préfixe dans lequel vous stockez les journaux de ce journal de suivi.
   - Chiffrement SSE-KMS des fichiers journaux : choisissez d'activer ou de désactiver le chiffrement des fichiers journaux avec SSE-KMS au lieu de SSE-S3.

- Validation du fichier journal : choisissez d'activer ou de désactiver la validation de l'intégrité des fichiers journaux.
- Livraison de notification SNS : choisissez d'activer ou de désactiver les notifications Amazon Simple Notification Service (Amazon SNS) selon lesquelles les fichiers journaux ont été livrés au compartiment spécifié pour le journal de suivi.

a. Pour transformer le suivi en suivi d' AWS Organizations organisation, vous pouvez choisir d'activer le suivi pour tous les comptes de votre organisation. Pour plus d'informations, consultez Création d'un journal de suivi pour une organisation.

b. Pour modifier le compartiment spécifié dans Emplacement de stockage, choisissez Création d'un compartiment S3 pour créer un compartiment. Lorsque vous créez un bucket, il CloudTrail crée et applique les politiques de bucket requises. Si vous choisissez de créer un nouveau compartiment S3, votre politique IAM doit inclure une autorisation pour l'`s3:PutEncryptionConfiguration`action, car le chiffrement côté serveur est activé par défaut pour le compartiment.

> **Note**
>
> Si vous avez choisi Utilisation du compartiment S3 existant, spécifiez un compartiment dans Nom du compartiment du journal de suivi, ou sélectionnez Parcourir pour choisir un compartiment. La politique du compartiment doit accorder CloudTrail l'autorisation d'y écrire. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.

Pour retrouver plus facilement vos journaux, créez un nouveau dossier (également appelé préfixe) dans un compartiment existant pour stocker vos CloudTrail journaux. Saisir le préfixe dans Préfixe.

c. Sous Chiffrement SSE-KMS du fichier journal, choisissez Activé si vous souhaitez chiffrer vos fichiers journaux avec SSE-KMS plutôt qu'avec SSE-S3. La valeur par défaut est Activé. Si vous n'activez pas le chiffrement SSE-KMS, vos journaux sont chiffrés à l'aide du chiffrement SSE-S3. Pour plus d'informations sur le chiffrement SSE-KMS, voir Utilisation du chiffrement côté serveur avec AWS Key Management Service (SSE-KMS). Pour plus d'informations sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3).

Si vous activez le chiffrement SSE-KMS, sélectionnez Nouveau ou Existant. AWS KMS key Dans AWS KMS Alias, spécifiez un alias au format `alias/MyAliasName`. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS. CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

> **Note**
>
> Vous pouvez également saisir l'ARN d'une clé à partir d'un autre compte. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS. La politique de clé doit CloudTrail autoriser l'utilisation de la clé pour chiffrer vos fichiers journaux et permettre aux utilisateurs que vous spécifiez de lire les fichiers journaux sous forme non chiffrée. Pour plus d'informations sur la modification manuelle de la politique de clés, consultez la page Configurer les politiques AWS KMS clés pour CloudTrail.

d. Dans Activer la validation du fichier journal, choisissez Oui pour que les fichiers de valeur de hachage des journaux soient livrés dans votre compartiment S3. Vous pouvez utiliser les fichiers de synthèse pour vérifier que vos fichiers journaux n'ont pas changé après leur CloudTrail livraison. Pour plus d'informations, consultez Validation de l' CloudTrail intégrité du fichier journal.

e. Pour l'envoi de notifications SNS, choisissez Enabled pour être averti chaque fois qu'un journal est envoyé à votre bucket. CloudTrail enregistre plusieurs événements dans un fichier journal. Des notifications SNS sont envoyées pour chaque fichier journal, non pour chaque événement. Pour plus d'informations, consultez Configuration des notifications Amazon SNS pour CloudTrail.

   Si vous activez les notifications SNS, pour Créer une nouvelle rubrique SNS, choisissez Nouveau pour créer une rubrique, ou Existant, pour utiliser une rubrique existante. Si vous créez un journal de suivi qui s'applique à toutes les régions, les notifications SNS relatives à la livraison de fichiers journaux de toutes les régions sont envoyées à la rubrique SNS unique que vous créez.

   Si vous choisissez Nouveau, vous CloudTrail spécifiez un nom pour le nouveau sujet ou vous pouvez saisir un nom. Si vous choisissez Existant, choisissez une rubrique SNS dans la liste déroulante. Vous pouvez également saisir l'ARN d'une rubrique provenant

d'une autre région ou d'un compte disposant des autorisations appropriées. Pour plus d'informations, consultez Politique relative aux rubriques Amazon SNS pour CloudTrail.

Si vous créez une rubrique, vous devez vous abonner à la rubrique pour être averti de l'envoi de fichiers journaux. Vous pouvez vous abonner à partir de la console Amazon SNS. En raison de la fréquence des notifications, nous vous recommandons de configurer l'abonnement pour pouvoir utiliser une file d'attente Amazon SQS afin de gérer les notifications par programmation. Pour plus d'informations, consultez Prise en main d'Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

4. Dans CloudWatch Logs, choisissez Modifier pour modifier les paramètres d'envoi des fichiers CloudTrail CloudWatch journaux vers Logs. Choisissez Activé dans CloudWatch les journaux pour activer l'envoi de fichiers journaux. Pour plus d'informations, consultez Envoyer des événements à CloudWatch Logs.

   a. Si vous activez l'intégration aux CloudWatch journaux, choisissez Nouveau pour créer un nouveau groupe de journaux ou Existant pour utiliser un groupe existant. Si vous choisissez Nouveau, vous CloudTrail spécifiez un nom pour le nouveau groupe de journaux ou vous pouvez saisir un nom.

   b. Si vous choisissez Existant, choisissez un groupe de journaux dans la liste déroulante.

   c. Choisissez Nouveau pour créer un nouveau rôle IAM afin d'obtenir les autorisations d'envoyer des CloudWatch journaux à Logs. Choisir Existant pour choisir un rôle IAM existant dans la liste déroulante. L'instruction de politique pour le rôle nouveau ou existant s'affiche lorsque vous déroulez Document de politique. Pour plus d'informations sur ce rôle, consultez Document de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance.

   > **Note**
   >
   > - Lorsque vous configurez un journal de suivi, vous pouvez choisir un compartiment S3 et une rubrique SNS qui appartiennent à un autre compte. Toutefois, si vous souhaitez CloudTrail transmettre des événements à un groupe de CloudWatch journaux journaux, vous devez choisir un groupe de journaux existant dans votre compte actuel.
   > - Seul le compte de gestion peut configurer un groupe de CloudWatch journaux pour un journal d'entreprise à l'aide de la console. L'administrateur délégué peut

configurer un groupe de CloudWatch journaux Logs à l'aide des opérations AWS CLI CloudTrail `CreateTrail` ou de `UpdateTrail` l'API.

5. Dans Balises, choisissez Modifier pour modifier, ajouter ou supprimer des identifications dans le journal de suivi. Ajoutez une ou plusieurs identifications personnalisées (paires clé-valeur) à votre journal de suivi. Les balises peuvent vous aider à identifier à la fois vos CloudTrail traces et les compartiments Amazon S3 contenant les fichiers CloudTrail journaux. Vous pouvez ensuite utiliser des groupes de ressources pour vos CloudTrail ressources. Pour plus d'informations, consultez AWS Resource Groups et Balises.
6. Dans Événements de gestion, choisissez Modifier pour modifier les paramètres de journalisation des événements de gestion.

   a. Pour Activité d'API, choisissez si vous souhaitez que votre journal d'activité journalise les événements Lire, Écrire ou les deux. Pour plus d'informations, consultez Événements de gestion.

   b. Choisissez Exclure les AWS KMS événements pour filtrer AWS Key Management Service (AWS KMS) les événements de votre parcours. Le paramètre par défaut est d'inclure tous les événements AWS KMS .

      L'option permettant d'enregistrer ou d'exclure AWS KMS des événements n'est disponible que si vous enregistrez des événements de gestion sur votre parcours. Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

      AWS KMS des actions telles que `EncryptDecrypt`, et génèrent `GenerateDataKey` généralement un grand volume (plus de 99 %) d'événements. Ces actions sont désormais journalisées en tant qu'événements Lecture. Les AWS KMS actions pertinentes à faible volume telles que `DisableDelete`, et `ScheduleKey` (qui représentent généralement moins de 0,5 % du volume d' AWS KMS événements) sont enregistrées en tant qu'événements d'écriture.

      Pour exclure les événements de volume important tels que `Encrypt`, `Decrypt` et `GenerateDataKey`, tout en continuant de journaliser les événements pertinents tels que `Disable`, `Delete` et `ScheduleKey`, choisissez de journaliser les événements de gestion Écriture et effacez la case à cocher pour Exclure les événements AWS KMS .

c. Choisissez Exclure les événements API de données Amazon RDS pour filtrer les événements d'API de données Amazon Relational Database Service Data hors de votre journal de suivi. Le paramètre par défaut consiste à inclure tous les événements d'API de données Amazon RDS. Pour plus d'informations sur les événements d'API Amazon RDS Data API, consultez Journalisation des appels d'API de données avec AWS CloudTrail dans le Guide de l'utilisateur Amazon RDS pour Aurora.

7. **Important**

   Les étapes 7 à 11 concernent la configuration des événements de données à l'aide de sélecteurs d'événements avancés. Les sélecteurs d'événements avancés vous permettent de configurer davantage de types d'événements de données et de contrôler avec précision les événements de données capturés par votre journal de suivi. Si vous utilisez des sélecteurs d'événements de base, veuillez consulter Mettre à jour les paramètres d'événements de données à l'aide de sélecteurs d'événements de base, puis revenez à l'étape 12 de cette procédure.

   Dans Événements de données, choisissez Modifier pour modifier les paramètres de journalisation des événements de données. Par défaut, les journaux de suivi ne journalisent pas les événements de données. Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour la tarification de CloudTrail, consultez Tarification d'AWS CloudTrail.

   Pour Type d'événement de données, choisissez le type de ressource sur lequel vous souhaitez journaliser les événements de données. Pour plus d'informations sur les types d'événements de données, veuillez consulter Événements de données.

   Note

   Pour enregistrer les événements de données pour AWS Glue les tables créées par Lake Formation, choisissez Lake Formation.

8. Choisissez un modèle de sélecteur de journaux. CloudTrail inclut des modèles prédéfinis qui enregistrent tous les événements de données pour le type de ressource. Pour créer un modèle de sélecteur de journal personnalisé, choisissez Personnaliser.

> **Note**
>
> Le choix d'un modèle prédéfini pour les compartiments S3 permet de consigner les événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois le suivi terminé. Il permet également de consigner l'activité liée aux événements de données effectuée par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
>
> Si le journal de suivi s'applique à une seule région, le fait de choisir un modèle prédéfini qui journalise tous les compartiments S3 permet la journalisation des événements de données pour tous les compartiments situés dans la même région que votre journal de suivi et tous les compartiments que vous créerez ultérieurement dans cette région. Il ne va pas journaliser les d'événements de données pour les compartiments Amazon S3 situés dans d'autres régions de votre compte AWS .
>
> Si vous créez un suivi pour toutes les régions, le choix d'un modèle prédéfini pour les fonctions Lambda permet de consigner les événements de données pour toutes les fonctions actuellement présentes dans votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans n'importe quelle région une fois le suivi créé. Si vous créez un suivi pour une seule région (à l'aide du AWS CLI), cette sélection active l'enregistrement des événements de données pour toutes les fonctions actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une fois que vous aurez fini de créer le journal. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions.
>
> La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectués par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

9. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.

10. Dans Sélecteurs d'événements avancés, créez une expression pour les ressources spécifiques sur lesquelles vous souhaitez collecter des événements de données. Vous pouvez ignorer cette étape si vous utilisez un modèle de journal prédéfini.

    a. Choisissez parmi les options suivantes.

    - **`readOnly`**- `readOnly` peut être défini pour être égal à une valeur de `true` ou`false`. Pour journaliser les deux événements `read` et `write`, n'ajoutez pas de sélecteur `readOnly`.
    - **`eventName`** - `eventName` peut utiliser n'importe quel opérateur. Vous pouvez l'utiliser pour inclure ou exclure tout événement de données enregistré CloudTrail, tel que `PutBucket` ou`GetSnapshotBlock`.
    - **`resources.ARN`**- Vous pouvez utiliser n'importe quel opérateur`resources.ARN`, mais si vous utilisez égal ou non, la valeur doit correspondre exactement à l'ARN d'une ressource valide du type que vous avez spécifié dans le modèle comme valeur de`resources.type`.

      Le tableau suivant affiche le format ARN valide de chaque `resources.type`.

      > **Note**
      >
      > Vous ne pouvez pas utiliser le `resources.ARN` champ pour filtrer les types de ressources dépourvus d'ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemake r: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Pour les tables ayant les flux activés, le champ `resources` dans l'événement de plan de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.

[2] Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante. La barre oblique de fin est intentionnelle ; ne l'excluez pas.

[3] Pour journaliser les événements sur tous les objets d'un point d'accès S3, il est recommandé d'utiliser uniquement l'ARN du point d'accès, de ne pas inclure le chemin d'accès de l'objet et d'utiliser les opérateurs `StartsWith` ou `NotStartsWith`.

Pour plus d'informations sur les formats ARN des ressources d'événements de données, consultez Actions, ressources et clés de condition dans le Guide de l'utilisateur AWS Identity and Access Management .

b. Pour chaque champ, choisissez + Conditions pour ajouter autant de conditions que vous le souhaitez, jusqu'à un maximum de 500 valeurs spécifiées pour toutes les conditions. Par exemple, pour exclure les événements de données de deux compartiments S3 des événements de données enregistrés sur votre parcours, vous pouvez définir le champ sur Resources.ARN, définir l'opérateur pour ne commence pas par, puis coller l'ARN d'un compartiment S3 ou rechercher les compartiments S3 pour lesquels vous ne souhaitez pas enregistrer d'événements.

   Pour ajouter le deuxième compartiment S3, choisissez + Conditions, puis répétez l'instruction précédente, en collant dans l'ARN ou en recherchant un compartiment différent.

   > **Note**
   >
   > Il est possible de définir un maximum de 500 valeurs pour tous les sélecteurs d'un journal de suivi. Cela inclut des tableaux de valeurs multiples pour un sélecteur tel que `eventName`. Si vous avez défini des valeurs uniques pour tous les sélecteurs, il est possible d'ajouter un maximum de 500 conditions à un sélecteur.
   > Si votre compte compte compte plus de 15 000 fonctions Lambda, vous ne pouvez pas afficher ou sélectionner toutes les fonctions dans la CloudTrail console lors de la création d'un journal. Il est toujours possible de journaliser toutes les fonctions à l'aide d'un modèle de sélecteur prédéfini, même si ces dernières ne sont pas affichées. Si vous souhaitez journaliser les événements de données de fonctions spécifiques, vous pouvez ajouter manuellement une fonction si vous connaissez son ARN. Vous pouvez également terminer la création du journal dans la console, puis utiliser la put-event-selectors commande AWS CLI et pour configurer la journalisation des événements de données pour des fonctions Lambda spécifiques. Pour plus d'informations, consultez Gérer les sentiers à l'aide du AWS CLI.

c. Choisir + champ pour ajouter des champs supplémentaires au besoin. Pour éviter les erreurs, il convient de ne pas définir de valeurs conflictuelles ou en double pour les champs. Par exemple, ne spécifiez pas un ARN dans un sélecteur pour être égal à une valeur, puis spécifiez que l'ARN n'est pas égal à la même valeur dans un autre sélecteur.

11. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données). Répétez les étapes de 3 à cette étape pour configurer les sélecteurs d'événements avancés pour le type d'événement de données.
12. Dans Événements Insights, choisissez Modifier si vous souhaitez que votre parcours enregistre les événements CloudTrail Insights.

    Dans Type d'événement, sélectionnez Événements Insights.

    Dans Événements Insights, choisissez Taux d'appels d'API,Taux d'erreurs d'API, ou les deux. Vous devez journaliser les événements de gestion Écriture pour journaliser les événements Insights afin de connaître le Taux d'appels d'API. Vous devez journaliser les événements de gestion Lecture ou Écriture pour journaliser les événements Insights afin de connaître le Taux d'erreur de l'API.

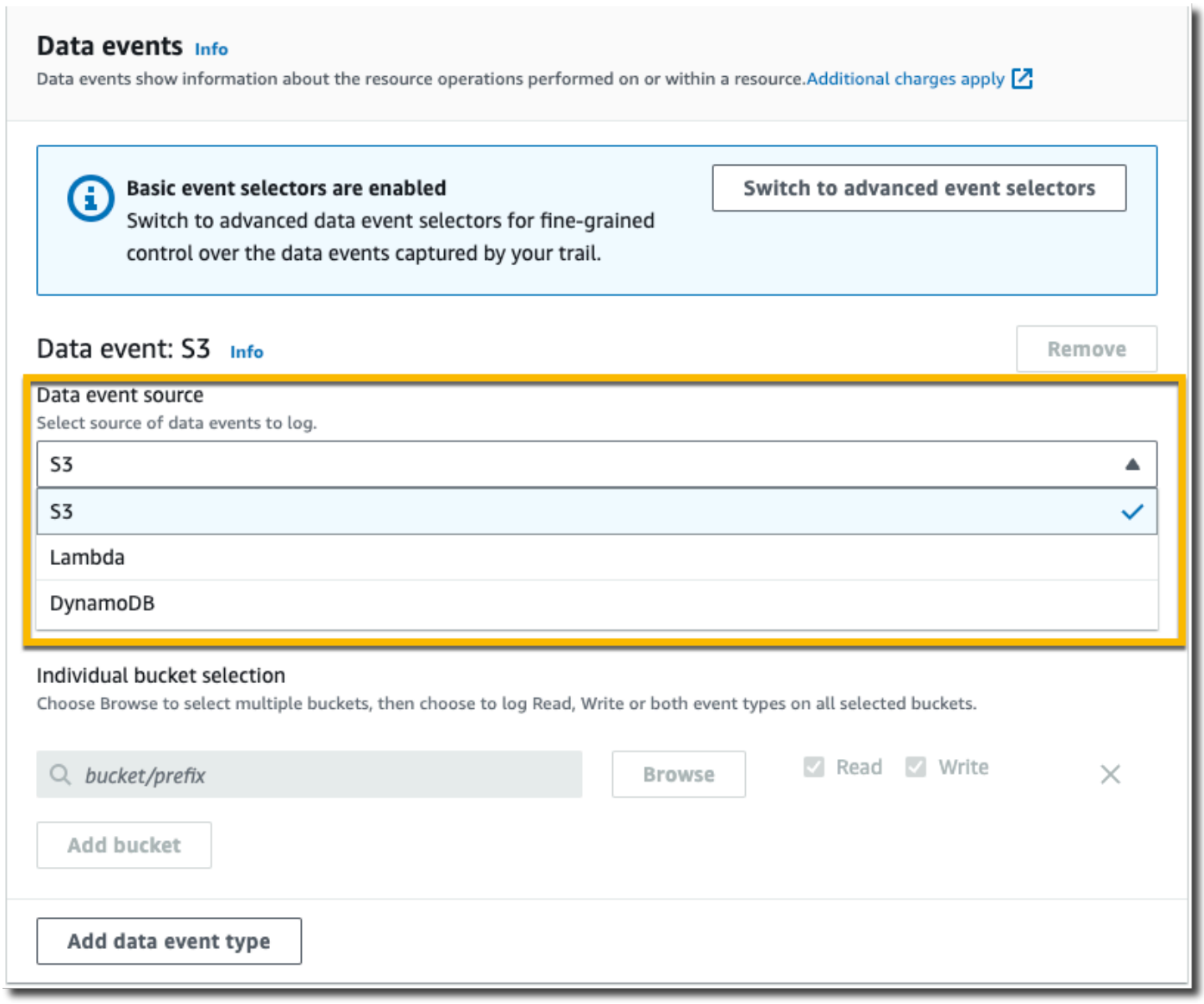
    CloudTrail Insights analyse les événements de gestion pour détecter toute activité inhabituelle et enregistre les événements lorsque des anomalies sont détectées. Par défaut, les journaux de suivi ne journalisent pas les événements Insights. Pour plus d'informations sur les événements Insights, consultez Journalisation des événements Insights. Des frais supplémentaires s'appliquent pour la journalisation des événements Insights. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

    Les événements Insights sont transmis à un dossier différent nommé `/CloudTrail-Insight` dans le même compartiment S3 spécifié dans la zone Emplacement de stockage de la page de détails du journal. CloudTrailcrée le nouveau préfixe pour vous. Par exemple, si votre compartiment S3 de destination actuel se nomme `S3bucketName/AWSLogs/CloudTrail/`, le nom du compartiment S3 avec un nouveau préfixe se nommera `S3bucketName/AWSLogs/CloudTrail-Insight/`.
13. Une fois que vous avez terminé de modifier les paramètres sur votre journal de suivi, choisissez Mettre à jour le journal d'activité.

Mettre à jour les paramètres d'événements de données à l'aide de sélecteurs d'événements de base

Vous pouvez utiliser des sélecteurs d'événements avancés pour configurer tous les types d'événements de données. Les sélecteurs d'événements avancés vous permettent de créer des sélecteurs précis pour enregistrer uniquement les événements qui vous intéressent.

Si vous utilisez des sélecteurs d'événements de base pour enregistrer des événements de données, vous êtes limité à la journalisation des événements de données pour les compartiments, les AWS Lambda fonctions et les tables Amazon DynamoDB d'Amazon S3. Vous ne pouvez pas filtrer sur le `eventName` terrain à l'aide de sélecteurs d'événements de base.



Utilisez la procédure suivante afin de configurer les paramètres des événements de données à l'aide de sélecteurs d'événements de base.

1. Dans Événements de données, choisissez Modifier pour modifier les paramètres de journalisation des événements de données. Avec les sélecteurs d'événements de base, vous pouvez spécifier des événements de données de journalisation pour les buckets Amazon S3, AWS Lambda les fonctions, les DynamoDBTables ou une combinaison de ces ressources.

Des types d'événements de données supplémentaires sont pris en charge avec des sélecteurs d'événements avancés. Par défaut, les journaux de suivi ne journalisent pas les événements de données. Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour plus d'informations, consultez Événements de données. Pour la tarification de CloudTrail, consultez Tarification d'AWS CloudTrail.

Pour les compartiments Amazon S3 :

a. Pour Data event source (Source d'événements de données), choisissez S3.

b. Il est possible de choisir de journaliser Tous les compartiments S3 actuels et futurs ou de spécifier des compartiments ou fonctions individuels. Par défaut, les événements de données sont journalisés pour tous les compartiments S3 actuels et futurs.

> **Note**
>
> Le maintien de l'option par défaut Tous les compartiments S3 actuels et futurs active la journalisation des événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois que vous avez terminé de créer le journal. Il permet également de consigner l'activité liée aux événements de données effectuée par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
> Si le journal de suivi s'applique à une seule région, le fait de choisir l'option Sélectionner tous les compartiments S3 de votre compte permet la journalisation des événements de données pour tous les compartiments situés dans la même région que votre journal de suivi et tous les compartiments que vous créerez ultérieurement dans cette région. Les événements de données relatifs aux compartiments Amazon S3 situés dans d'autres régions ne seront pas enregistrés dans votre AWS compte.

c. Si vous laissez l'option par défaut, Tous les compartiments S3 actuels et futurs, choisissez de journaliser les événements de lecture, les événements d'écriture, ou les deux.

d. Pour sélectionner des compartiments individuels, il convient de vider les boîtes de dialogue Lecture et Écriture pour Tous les compartiments S3 actuels et futurs. Dans Sélection du compartiment individuel, recherchez un compartiment sur lequel journaliser les événements de données. Pour rechercher des compartiments spécifiques, tapez un préfixe de compartiment pour le compartiment souhaité. Il est possible de sélectionner plusieurs

compartiments dans cette fenêtre. Choisissez Ajouter un compartiment pour journaliser les événements de données pour d'autres compartiments. Choisissez de journaliser les événements Lecture tels que `GetObject`, les événements Écriture tels que `PutObject`, ou les deux.

Ce paramètre est prioritaire par rapport aux paramètres que vous définissez pour les compartiments individuels. Par exemple, si vous spécifiez la journalisation des événements Read (Lecture) pour tous les compartiments S3, puis choisissez d'ajouter un compartiment spécifique pour la journalisation des événements de données, Read (Lecture) est déjà sélectionné pour le compartiment que vous avez ajouté. Vous ne pouvez pas effacer la sélection. Vous pouvez uniquement configurer l'option pour Écriture.

Pour supprimer un compartiment de la journalisation, choisissez X.

2. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données).
3. Pour les fonctions Lambda :

   a. Pour Data event source (Source d'événement de données), choisissez Lambda.

   b. Dans Fonction Lambda, choisissez Toutes les régions pour journaliser toutes les fonctions Lambda, ou Fonction d'entrée en tant qu'ARN, pour consigner les événements de données sur une fonction spécifique.

   Pour enregistrer les événements de données relatifs à toutes les fonctions Lambda de votre AWS compte, sélectionnez Enregistrer toutes les fonctions actuelles et futures. Ce paramètre est prioritaire par rapport aux paramètres que vous définissez pour les fonctions individuelles. Toutes les fonctions sont journalisées, même si elles ne sont pas toutes affichées.

   > **Note**
   >
   > Si vous créez un suivi pour toutes les régions, cette sélection active l'enregistrement des événements de données pour toutes les fonctions actuellement présentes dans votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans n'importe quelle région une fois que vous aurez fini de créer le journal. Si vous créez un suivi pour une seule région (à l'aide du AWS CLI), cette sélection active l'enregistrement des événements de données pour toutes les fonctions actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une

fois que vous aurez fini de créer le journal. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions. La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectués par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

c. Si vous choisissez Fonction d'entrée en tant qu'ARN, saisissez l'ARN d'une fonction Lambda.

> **Note**
>
> Si votre compte compte compte plus de 15 000 fonctions Lambda, vous ne pouvez pas afficher ou sélectionner toutes les fonctions dans la CloudTrail console lors de la création d'un journal. Vous pouvez toujours sélectionner l'option de journalisation de toutes les fonctions, même si elles ne sont pas affichées. Si vous souhaitez journaliser les événements de données de fonctions spécifiques, vous pouvez ajouter manuellement une fonction si vous connaissez son ARN. Vous pouvez également terminer la création du journal de suivi dans la console, puis utiliser la AWS CLI et la commande put-event-selectors afin de configurer la journalisation d'événements de données pour des fonctions Lambda spécifiques. Pour plus d'informations, consultez Gérer les sentiers à l'aide du AWS CLI.

4. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données).
5. Pour les tables DynamoDB :

   a. Pour Data event source (Source d'événement de données), choisissez DynamoDB.

   b. Dans DynamoDB table selection (Sélection d'une table DynamoDB), choisissez Browse (Parcourir) pour sélectionner une table ou coller dans l'ARN d'une table DynamoDB à laquelle vous avez accès. Un ARN de table DynamoDB se présente sous le format suivant :

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   Pour ajouter une autre table, choisissez Ajouter une ligne, puis recherchez un tableau ou collez dans l'ARN d'une table à laquelle vous avez accès.

6. Pour configurer les événements Insights et d'autres paramètres pour votre piste, revenez à la procédure précédente dans cette rubrique, Mise à jour d'un journal de suivi.

Suppression d'un journal de suivi

Vous pouvez supprimer des pistes à l'aide de la CloudTrail console. Si le compte de gestion ou le compte d'administrateur délégué d'une organisation supprime un journal de suivi de l'organisation, le journal est supprimé de tous les comptes membres de l'organisation.

Si vous avez activé les événements CloudTrail de gestion dans Amazon Security Lake, vous devez gérer au moins un journal organisationnel multirégional qui enregistre à la fois les `read` événements de gestion et les événements `write` de gestion. Vous ne pouvez pas supprimer une piste si c'est la seule qui répond à cette exigence, sauf si vous désactivez les événements CloudTrail de gestion dans Security Lake.

Pour supprimer une trace à l'aide de la CloudTrail console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Ouvrez la page Trails de la CloudTrail console.
3. Choisissez le nom du journal de suivi.
4. En haut de la page des détails du journal de suivi, choisissez Delete (Supprimer).
5. Lorsque vous êtes invité à confirmer la suppression, choisissez Delete (Supprimer) pour supprimer le journal de suivi de manière définitive. Le journal de suivi sera supprimé de la liste des journaux de suivi pour la région. Les fichiers journaux déjà livrés au compartiment Amazon S3 ne sont pas supprimés.

> **Note**
>
> Le contenu livré aux compartiments Amazon S3 peut contenir du contenu client. Pour plus d'informations sur la suppression de données sensibles, consultez les sections Vidage d'un compartiment et Suppression d'un compartiment dans le guide de l'utilisateur Amazon S3.

Désactivation de la journalisation pour un journal d'activité

Lorsque vous créez un journal d'activité, la journalisation est activée automatiquement. Vous pouvez désactiver la journalisation d'activité.

Lorsque vous désactivez la journalisation, les journaux existants sont toujours stockés dans le compartiment Amazon S3 pour le suivi et continuent d'entraîner des frais S3.

Pour désactiver la journalisation d'un parcours à l'aide de la CloudTrail console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation de gauche, choisissez Trails (Journaux d'activité), puis le nom du journal d'activité.
3. En haut de la page détaillée du journal d'activité, choisissez Stop logging (Arrêter la journalisation) pour désactiver la journalisation du journal d'activité.
4. Lorsque vous êtes invité à confirmer, choisissez Arrêter la journalisation. CloudTrailarrête l'activité d'enregistrement pour ce sentier.
5. Pour reprendre la journalisation pour ce journal d'activité, choisissez Start logging (Démarrer la journalisation) sur la page de configuration du journal d'activité.

Création, mise à jour et gestion de sentiers à l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour créer, mettre à jour et gérer vos sentiers. Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la AWS région configurée pour votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

> **Note**
>
> Vous avez besoin des outils de ligne de AWS commande pour exécuter les commandes AWS Command Line Interface (AWS CLI) de cette rubrique. Assurez-vous d'avoir AWS CLI installé une version récente du. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Command Line Interface. Pour obtenir de l'aide CloudTrail concernant les commandes en ligne de AWS CLI commande, tapez`aws cloudtrail help`.

Commandes généralement utilisées pour la création, la gestion et l'état d'un journal de suivi

Parmi les commandes les plus couramment utilisées pour créer et mettre à jour des sentiers, CloudTrail citons :

- create-trail pour créer un journal de suivi.
- update-trail pour modifier la configuration d'un journal de suivi existant.
- add-tags pour ajouter une ou plusieurs identifications (paires clé-valeur) à un journal de suivi existant.
- remove-tags pour supprimer une ou plusieurs identifications d'un journal de suivi.
- list-tags pour renvoyer une liste des identifications associées à un journal de suivi.
- put-event-selectors pour ajouter ou modifier des sélecteurs d'événements pour un journal de suivi.
- put-insight-selectors pour ajouter ou modifier des sélecteurs d'événements Insights pour un journal de suivi existant, et activer ou désactiver les événements Insights.
- start-logging pour commencer la journalisation des événements avec votre journal de suivi.
- stop-logging pour interrompre la journalisation des événements avec votre journal de suivi.
- delete-trail pour supprimer un journal de suivi. Cette commande ne supprime pas le compartiment Amazon S3 qui contient les fichiers journaux pour ce journal de suivi, le cas échéant.
- describe-trailspour renvoyer des informations sur les sentiers d'une AWS région.
- get-trail pour renvoyer les informations sur les paramètres d'un journal de suivi.
- get-trail-status pour renvoyer des informations sur l'état actuel d'un journal de suivi.
- get-event-selectors pour renvoyer des informations sur les sélecteurs d'événements configurés pour un journal de suivi.
- get-insight-selectors pour renvoyer des informations sur les sélecteurs d'événements Insights configurés pour un journal de suivi.

Les commandes prises en charge pour la création et la mise à jour de journaux de suivi: create-trail et update-trail

Les commandes `create-trail` et `update-trail` offrent une variété de fonctionnalités pour la création et la gestion des journaux de suivi, y compris:

- Créer un journal de suivi qui reçoit des journaux entre les régions, ou mettre à jour un journal de suivi avec l'option `--is-multi-region-trail`. Dans la plupart des cas, vous devez créer des sentiers qui enregistrent les événements dans toutes les AWS régions.
- Création d'un journal qui reçoit les journaux de tous les AWS comptes d'une organisation avec l'`--is-organization-trail`option.
- Convertir un journal de suivi multi-régions en un journal suivi à région unique avec l'option `--no-is-multi-region-trail`.
- Activer ou désactiver le chiffrement des fichiers journaux avec l'option `--kms-key-id`. L'option indique une AWS KMS clé que vous avez déjà créée et à laquelle vous avez attaché une politique qui permet CloudTrail de chiffrer vos journaux. Pour plus d'informations, consultez Activation et désactivation du chiffrement des fichiers CloudTrail journaux à l'aide du AWS CLI.
- Activer ou désactiver la validation de fichiers journaux avec les options `--no-enable-log-file-validation` et `--enable-log-file-validation`. Pour plus d'informations, consultez Validation de l' CloudTrail intégrité du fichier journal.
- Spécification d'un groupe de CloudWatch journaux et d'un rôle CloudTrail permettant de transmettre des événements à un groupe de CloudWatch journaux de journaux. Pour plus d'informations, consultez Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.

Commandes obsolètes: create-subscription et update-subscription

> **Important**
>
> Les commandes `create-subscription` et `update-subscription` ont été utilisées pour créer et mettre à jour des journaux de suivi, mais sont obsolètes. N'utilisez pas ces commandes. Elles n'offrent pas de fonctionnalités complètes pour la création et la gestion des journaux de suivi.
>
> Si vous avez configuré une automatisation qui utilise une ou deux de ces commandes, nous vous recommandons de mettre à jour votre code ou vos scripts pour utiliser les commandes prises en charge, par exemple create-trail.

Utilisation de create-trail

Vous pouvez utiliser la commande `create-trail` pour créer des journaux de suivi qui sont spécifiquement configurés pour répondre aux besoins de votre entreprise. Lorsque vous utilisez

le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la AWS région configurée pour votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

Création d'un journal de suivi qui s'applique à toutes les régions

Pour créer un journal de suivi qui s'applique à toutes les régions, utilisez l'option `--is-multi-region-trail`. Par défaut, la commande `create-trail` crée un journal de suivi qui journalise les événements uniquement dans la région AWS dans laquelle le journal de suivi a été créé. Pour vous assurer de consigner les événements de service mondiaux et de capturer toutes les activités liées à la gestion des événements dans votre AWS compte, vous devez créer des traces qui enregistrent les événements dans toutes les AWS régions.

> **Note**
>
> Lorsque vous créez un suivi, si vous spécifiez un compartiment Amazon S3 qui n'a pas été créé avec CloudTrail, vous devez joindre la politique appropriée. Consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.

L'exemple suivant crée un journal de suivi avec le nom *my-trail* et une identification avec une clé nommée *Groupe* avec une valeur *Marketing* qui livre des journaux de toutes les régions à un compartiment préexistant nommé *my-bucket*.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

Afin de confirmer que votre journal de suivi existe dans toutes les régions, l'élément `IsMultiRegionTrail` du résultat affiche `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Utilisez la commande `start-logging` pour démarrer la journalisation pour votre journal de suivi.

Démarrer la journalisation pour le journal de suivi

Une fois la commande `create-trail` terminée, exécutez la commande `start-logging` pour démarrer la journalisation pour ce journal de suivi.

> **Note**
>
> Lorsque vous créez un parcours avec la CloudTrail console, la journalisation est automatiquement activée.

L'exemple suivant démarre la journalisation pour un journal de suivi.

```
aws cloudtrail start-logging --name my-trail
```

Cette commande ne renvoie pas de résultat, mais vous pouvez utiliser la commande `get-trail-status` pour vérifier que la journalisation a démarré.

```
aws cloudtrail get-trail-status --name my-trail
```

Afin de confirmer que le journal de suivi réalise la journalisation, l'élément `IsLogging` dans le résultat affiche `true`.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
```

```
    "TimeLoggingStopped": ""
}
```

Créer un journal de suivi à région unique

La commande suivante crée un journal de suivi à région unique. Le compartiment Amazon S3 spécifié doit déjà exister et les CloudTrail autorisations appropriées doivent être appliquées. Pour plus d'informations, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

Pour plus d'informations, consultez Exigences de dénomination.

Voici un exemple de sortie.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Créer un journal de suivi qui s'applique à toutes les régions et ayant la validation de fichiers journaux activée

Pour activer la validation du fichier journal lorsque vous utilisez `create-trail`, utilisez l'option `--enable-log-file-validation`.

Pour plus d'informations sur la validation de fichiers journaux, consultez Validation de l' CloudTrail intégrité du fichier journal.

L'exemple suivant crée un journal de suivi qui livre des journaux de toutes les régions au compartiment spécifié. La commande utilise l'option `--enable-log-file-validation`.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --enable-log-file-validation
```

Afin de confirmer que la validation de fichiers journaux est activée, l'élément `LogFileValidationEnabled` dans le résultat affiche `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Utilisation d'update-trail

> **Important**
>
> Depuis le 22 novembre 2021, la façon dont les sentiers capturent les événements liés au service mondial AWS CloudTrail a changé. Désormais, les événements créés par Amazon CloudFront AWS STS sont enregistrés dans la région dans laquelle ils ont été créés, la région USA Est (Virginie du Nord), us-east-1. AWS Identity and Access Management Cela rend le CloudTrail traitement de ces services cohérent avec celui des autres services AWS mondiaux. Pour continuer à recevoir les événements de service global en dehors des USA Est (Virginie du Nord), veillez à convertir les journaux de suivi à région unique utilisant des événements de services mondiaux en dehors des USA Est (Virginie du Nord) en journaux de suivi multi-régions. Pour plus d'informations sur la capture des événements de services mondiaux, consultez Activation et désactivation de la journalisation des événements de services mondiaux plus loin dans cette section.
> En revanche, l'historique des événements de la CloudTrail console et la aws cloudtrail lookup-events commande afficheront ces événements Région AWS là où ils se sont produits.

Vous pouvez utiliser la commande `update-trail` pour modifier les paramètres de configuration d'un journal de suivi. Vous pouvez également utiliser les commandes add-tags et remove-tags pour ajouter et supprimer les identifications pour un journal de suivi. Vous ne pouvez mettre à jour les sentiers que depuis la AWS région où ils ont été créés (sa région d'origine). Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la AWS région configurée pour

votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

Si vous avez activé les événements CloudTrail de gestion dans Amazon Security Lake, vous devez gérer au moins un journal organisationnel multirégional qui enregistre à la fois les `read` événements de gestion et les événements `write` de gestion. Vous ne pouvez pas mettre à jour un journal de suivi éligible de telle sorte qu'il ne réponde pas aux exigences de Security Lake. Par exemple, en modifiant le journal de suivi pour qu'il s'applique à une région unique ou en désactivant la journalisation des événements de gestion `read` et `write`.

> **Note**
>
> Si vous utilisez le AWS CLI ou l'un des AWS SDK pour modifier un parcours, assurez-vous que la politique de compartiment du parcours est up-to-date conforme. Pour que votre bucket reçoive automatiquement les événements d'un nouveau Région AWS, la politique doit contenir le nom complet du service,`cloudtrail.amazonaws.com`. Pour plus d'informations, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.

Rubriques

Convertir un journal de suivi qui s'applique à une région de sorte qu'il s'applique à toutes les régions

Pour modifier un journal de suivi existant afin qu'il s'applique à toutes les régions, utilisez l'option `--is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Afin de confirmer que le journal de suivi s'applique maintenant à toutes les régions, l'élément `IsMultiRegionTrail` dans le résultat affiche `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Convertir un journal de suivi multi-régions à un journal de suivi à région unique

Pour modifier un journal de suivi multi-régions existant afin qu'il s'applique uniquement à la région dans laquelle il a été créé, utilisez l'option `--no-is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

Afin de confirmer que le journal de suivi s'applique maintenant à une seule région, l'élément `IsMultiRegionTrail` dans le résultat affiche `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Activation et désactivation de la journalisation des événements de services mondiaux

Pour modifier un journal de suivi afin qu'il ne journalise pas les événements de services mondiaux, utilisez l'option `--no-include-global-service-events`.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

Pour confirmer que le journal de suivi ne journaliser plus d'événements de services mondiaux, l'élément `IncludeGlobalServiceEvents` dans le résultat indique `false`.

```
{
```

```
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Pour modifier un journal de suivi afin qu'il journalise les événements de services mondiaux, utilisez l'option `--include-global-service-events`.

Les journaux de suivi à région unique ne recevront plus d'événements de services mondiaux à partir du 22 novembre 2021, sauf si le journal de suivi apparaît déjà dans la région USA Est (Virginie du Nord), us-east-1. Pour continuer à capturer les événements de services mondiaux, mettez à jour la configuration du journal de suivi en un journal de suivi multi-régions. Par exemple, cette commande met à jour un journal de suivi à région unique dans USA Est (Ohio), us-east-2, en un journal de suivi multi-régions. Remplacez *myExistingSingleRegionTrailWithGSE* par le nom de piste approprié à votre configuration.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

Étant donné que les activités de services mondiaux ne sont disponibles dans la région USA Est (Virginie du Nord) qu'à partir du 22 novembre 2021, vous pouvez également créer un journal de suivi à région unique pour vous abonner aux activités de services mondiaux dans la région USA Est (Virginie du Nord), us-east-1. La commande suivante crée un suivi régional unique dans us-east-1 pour la réception, l'IAM et les CloudFront événements : AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

Activer la validation du fichier journal

Pour activer la validation du fichier journal pour un journal de suivi, utilisez l'option `--enable-log-file-validation`. Les fichiers de valeur de hachage sont livrés au compartiment Amazon S3 pour ce journal de suivi.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

Afin de confirmer que la validation de fichiers journaux est activée, l'élément `LogFileValidationEnabled` dans le résultat affiche `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Désactiver la validation du fichier journal

Pour désactiver la validation du fichier journal pour un journal de suivi, utilisez l'option `--no-enable-log-file-validation`.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

Afin de confirmer que la validation du fichier journal est désactivée, l'élément `LogFileValidationEnabled` dans le résultat affiche `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Pour valider les fichiers journaux avec AWS CLI le[Validation de l'intégrité du fichier CloudTrail journal à l'aide du AWS CLI](#).

Gérer les sentiers à l'aide du AWS CLI

AWS CLI Il inclut plusieurs autres commandes qui vous aident à gérer vos sentiers. Ces commandes ajoutent des identifications aux journaux de suivi pour obtenir le statut du journal de suivi, démarrer

et arrêter la journalisation pour les journaux de suivi et supprimer un journal de suivi. Vous devez exécuter ces commandes depuis la même AWS région où le parcours a été créé (sa région d'origine). Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la AWS région configurée pour votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre --region avec la commande.

Rubriques

Ajouter une ou plusieurs identifications à un journal de suivi

Pour ajouter une ou plusieurs identifications à un journal de suivi existant, utilisez la commande add-tags.

L'exemple suivant ajoute une identification avec le nom *Owner* (Propriétaire) et la valeur de *Mary* à un journal de suivi avec l'ARN de *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* dans la région USA Est (Ohio).

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

Si elle aboutit, cette commande ne renvoie rien.

Liste des identifications pour un ou plusieurs journaux de suivi

Pour afficher les identifications associées à un ou plusieurs journaux de suivi existants, utilisez la commande list-tags.

L'exemple suivant répertorie les identifications pour *Trail1* et *Trail2*.

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

Si elle aboutit, cette commande renvoie un résultat similaire à ce qui suit.

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "Name"
             },
             {
                 "Value": "Ohio",
                 "Key": "Location"
             }
         ]
     },
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
         "TagsList": [
             {
                 "Value": "Bob",
                 "Key": "Name"
             }
         ]
     }
  ]
}
```

Supprimer une ou plusieurs identifications à partir d'un journal de suivi

Pour supprimer une ou plusieurs identifications d'un journal de suivi existant, utilisez la commande remove-tags.

L'exemple suivant supprime les identifications avec les noms *Location* (Emplacement) et *Name* (Nom) d'un journal de suivi avec l'ARN de *arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1* dans la région USA Est (Ohio).

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

Si elle aboutit, cette commande ne renvoie rien.

Récupération des paramètres et de l'état d'un journal de suivi

Exécutez la `describe-trails` commande pour récupérer des informations sur les sentiers d'une AWS région. L'exemple suivant renvoie des informations sur les journaux de suivi configurés dans la région USA Est (Ohio).

```
aws cloudtrail describe-trails --region us-east-2
```

Si la commande aboutit, vous obtenez un résultat similaire à ce qui suit.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
```

```
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
    }
  ]
}
```

Utilisez la commande `get-trail` pour récupérer les informations sur les paramètres d'un journal de suivi spécifique. L'exemple suivant renvoie les informations sur les paramètres d'un journal de suivi nommé *my-trail*.

```
aws cloudtrail get-trail - -name my-trail
```

Si elle aboutit, cette commande renvoie un résultat similaire à ce qui suit.

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

Exécutez la commande `get-trail-status` pour récupérer l'état d'un journal de suivi. Vous devez exécuter cette commande depuis la AWS région dans laquelle elle a été créée (la région d'origine) ou vous devez spécifier cette région en ajoutant le --region paramètre.

> **Note**
>
> Si le parcours est un parcours organisé par une organisation et que vous êtes un compte membre de l'organisation dans AWS Organizations, vous devez fournir l'ARN complet de ce parcours, et pas seulement son nom.

```
aws cloudtrail get-trail-status --name my-trail
```

Si la commande aboutit, vous obtenez un résultat similaire à ce qui suit.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Outre les champs affichés dans le code JSON précédent, l'état contient les champs suivants si des erreurs sont survenues dans Amazon SNS ou Amazon S3 :

- `LatestNotificationError`. Contient l'erreur émise par Amazon SNS en cas d'échec d'un abonnement à une rubrique.
- `LatestDeliveryError`. Contient l'erreur émise par Amazon S3 en cas d' CloudTrail impossibilité de fournir un fichier journal à un compartiment.

Configuration des sélecteurs d'événements CloudTrail Insights

Activez les événements Insights sur un journal de suivi en exécutant put-insight-selectors, et en spécifiant `ApiCallRateInsight`, `ApiErrorRateInsight`, ou les deux comme valeur de `InsightType` l'attribut . Pour afficher les paramètres du sélecteur Insights pour un journal de suivi, exécutez la commande `get-insight-selectors`. Vous devez exécuter cette commande depuis la AWS région dans laquelle le parcours a été créé (la région d'origine) ou vous devez spécifier cette région en ajoutant le --region paramètre à la commande.

> **Note**
>
> Pour journaliser les événements Insights pour `ApiCallRateInsight`, le journal de suivi doit journaliser les événements de gestion `write`. Pour journaliser les événements Insights pour `ApiErrorRateInsight`, le journal de suivi doit journaliser les événements de gestion `read` ou `write`.

Exemple : un journal de suivi qui journalise les événements Insights

L'exemple suivant permet put-insight-selectors de créer un sélecteur d'événements Insights pour un parcours nommé *`TrailName3`*. Cela permet de collecter des événements Insights pour le parcours *`TrailName3`*. Le sélecteur d'événements Insights journalise les deux `ApiErrorRateInsight` et `ApiCallRateInsight`Types d'événements Insights.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

L'exemple montre comment renvoyer le sélecteur d'événements Insights configuré pour le journal de suivi.

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
```

```
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Exemple: désactiver la collecte d'événements Insights pour un journal de suivi

L'exemple suivant permet put-insight-selectors de supprimer le sélecteur d'événements Insights pour une piste nommée *TrailName3*. La suppression de la chaîne JSON des sélecteurs Insights désactive la collecte d'événements Insights pour le trail *TrailName3*.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

L'exemple renvoie le sélecteur d'événement Insights maintenant vide configuré pour le journal de suivi.

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Configuration des sélecteurs d'événements

Pour afficher les paramètres du sélecteur d'événements pour un journal de suivi, exécutez la commande `get-event-selectors`. Vous devez exécuter cette commande depuis la AWS région dans laquelle elle a été créée (la région d'origine) ou vous devez spécifier cette région à l'aide du --region paramètre.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Si le parcours est un parcours organisé par une organisation et que vous êtes un compte membre de l'organisation dans AWS Organizations, vous devez fournir l'ARN complet de ce parcours, et pas seulement son nom.

L'exemple suivant renvoie les paramètres par défaut pour un sélecteur d'événements pour un journal de suivi.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour créer un sélecteur d'événements, exécutez la commande `put-event-selectors`. Si vous souhaitez journaliser les événements Insights sur le journal de suivi, assurez-vous que le sélecteur d'événements active la journalisation des types Insights pour lesquels vous souhaitez configurer votre journal de suivi. Pour plus d'informations sur la journalisation des événements Insights, veuillez consulter Journalisation des événements Insights.

Lorsqu'un événement se produit dans votre compte, CloudTrail évalue la configuration de vos sentiers. Si l'événement correspond à un sélecteur d'événements pour un journal de suivi, il est traité et journalisé par le journal de suivi. Vous pouvez configurer jusqu'à 5 sélecteurs d'événements et jusqu'à 250 ressources de données pour un journal de suivi. Pour plus d'informations, consultez Journalisation des événements de données.

Rubriques

- Exemple: journal de suivi avec sélecteurs d'événements spécifiques
- Exemple: journal de suivi qui journalise tous les événements de gestion et de données
- Exemple de parcours qui n'enregistre pas AWS Key Management Service les événements
- Exemple de journal qui enregistre les événements pertinents à faible volume AWS Key Management Service
- Exemple de journal de suivi qui ne journalise pas les événements d'API de données Amazon RDS

Exemple: journal de suivi avec sélecteurs d'événements spécifiques

L'exemple suivant crée un sélecteur d'événements pour un journal nommé *`TrailName`*afin d'inclure des événements de gestion en lecture seule et en écriture seule, des événements de données pour deux combinaisons de compartiments et de préfixes Amazon S3 et des événements de données pour une seule fonction nommée. AWS Lambda *`hello-world-python-function`*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix","arn:aws:s3:::mybucket2/prefix2"]},{"Type": "AWS::Lambda::Function","Values":
 ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]}]}]'
```

L'exemple renvoie le sélecteur d'événements configuré pour le journal de suivi.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Exemple: journal de suivi qui journalise tous les événements de gestion et de données

L'exemple suivant crée un sélecteur d'événements pour une piste nommée *TrailName2* qui inclut tous les événements, y compris les événements de gestion en lecture seule et en écriture seule, ainsi que tous les événements de données pour tous les compartiments, fonctions AWS Lambda et tables Amazon DynamoDB d'Amazon S3 du compte. AWS Comme cet exemple utilise des sélecteurs d'événements de base, il ne peut pas configurer la journalisation des événements S3 sur

AWS Outposts, des appels Amazon Managed Blockchain JSON-RPC sur des nœuds Ethereum ou d'autres types de ressources de sélection d'événements avancés. Vous devez utiliser des sélecteurs d'événements avancés pour journaliser les événements de données de ces ressources. Pour plus d'informations, consultez Configuration des sélecteurs d'événements avancés.

> **Note**
>
> Si le journal de suivi s'applique à une seule région, seuls les événements de cette région sont consignés, même si les paramètres du sélecteur d'événements spécifient tous les compartiments Amazon S3 et fonctions Lambda. Les sélecteurs d'événements s'appliquent uniquement aux régions dans lesquelles le journal de suivi est créé.

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

L'exemple renvoie les sélecteurs d'événements configurés pour le journal de suivi.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
```

```
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

Exemple de parcours qui n'enregistre pas AWS Key Management Service les événements

L'exemple suivant crée un sélecteur d'événements pour un journal nommé *TrailName*pour inclure les événements de gestion en lecture seule et en écriture seule, mais pour exclure les événements (). AWS Key Management Service AWS KMSÉtant donné que les AWS KMS événements sont traités comme des événements de gestion et qu'ils peuvent être nombreux, ils peuvent avoir un impact important sur votre CloudTrail facture si vous disposez de plusieurs pistes qui enregistrent les événements de gestion. Dans cet exemple, l'utilisateur a choisi d'exclure les événements AWS KMS de chaque journal de suivi, sauf un. Pour exclure une source d'événement, ajoutez `ExcludeManagementEventSources` à vos sélecteurs d'événements et spécifiez une source d'événement dans la valeur de chaîne.

Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

Pour recommencer à AWS KMS consigner les événements dans un journal, transmettez un tableau vide comme valeur de`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

L'exemple renvoie le sélecteur d'événements configuré pour le journal de suivi.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
```

```
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour recommencer à consigner les AWS KMS événements dans un journal, transmettez un tableau vide comme valeur de`ExcludeManagementEventSources`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Exemple de journal qui enregistre les événements pertinents à faible volume AWS Key Management Service

L'exemple suivant crée un sélecteur d'événements pour un parcours nommé de manière *TrailName*à inclure des événements de gestion en écriture seule et des événements. AWS KMS Étant donné que les AWS KMS événements sont traités comme des événements de gestion et qu'ils peuvent être nombreux, ils peuvent avoir un impact important sur votre CloudTrail facture si vous disposez de plusieurs pistes qui enregistrent les événements de gestion. Dans cet exemple, l'utilisateur a choisi d'inclure les événements AWS KMS Write, qui incluront `DisableScheduleKey`, `Delete` mais n'incluront plus les actions à volume élevé telles que `EncryptDecrypt`, et `GenerateDataKey` (elles sont désormais traitées comme des événements de lecture).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

L'exemple renvoie le sélecteur d'événements configuré pour le journal de suivi. Cela enregistre les événements de gestion en écriture uniquement, y compris AWS KMS les événements.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
```

```
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Exemple de journal de suivi qui ne journalise pas les événements d'API de données Amazon RDS

L'exemple suivant crée un sélecteur d'événements pour un journal nommé *TrailName*pour inclure les événements de gestion en lecture seule et en écriture seule, mais pour exclure les événements de l'API Amazon RDS Data. Étant donné que les événements de l'API Amazon RDS Data sont traités comme des événements de gestion et qu'ils peuvent être très nombreux, ils peuvent avoir un impact important sur votre CloudTrail facture si vous disposez de plusieurs traces qui capturent les événements de gestion. Dans cet exemple, l'utilisateur a choisi d'exclure les événements d'API de données Amazon RDS de chaque journal de suivi, sauf un. Pour exclure une source d'événement, ajoutez `ExcludeManagementEventSources` à vos sélecteurs d'événements et spécifiez une source d'événement d'API de données Amazon RDS dans la valeur de chaîne : `rdsdata.amazonaws.com`.

Si vous choisissez de ne pas journaliser les événements de gestion, les événements d'API de données Amazon RDS ne seront pas journalisés et vous ne pourrez pas modifier les paramètres de journalisation des événements.

Pour recommencer à consigner les événements de gestion de l'API Amazon RDS Data dans un journal, transmettez un tableau vide comme valeur de`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

L'exemple renvoie le sélecteur d'événements configuré pour le journal de suivi.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
```

```
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour recommencer à consigner les événements de gestion de l'API Amazon RDS Data dans un journal, transmettez un tableau vide comme valeur de`ExcludeManagementEventSources`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Configuration des sélecteurs d'événements avancés

Pour utiliser des sélecteurs d'événements avancés pour inclure ou exclure des événements de données au lieu des sélecteurs d'événements de base, optez pour utiliser des sélecteurs d'événements avancés sur la page de détails d'une piste. Les sélecteurs d'événements avancés vous permettent de journaliser des événements de données sur davantage de types de ressources que les sélecteurs d'événements de base. Les sélecteurs de base journalisent l'activité des objets S3, l'activité d'exécution des fonctions AWS Lambda et les tables DynamoDB.

Dans les sélecteurs d'événements avancés, créez une expression pour collecter des événements de données sur des types de ressources spécifiques tels que les compartiments S3, les AWS Lambda fonctions, les tables DynamoDB, les points d'accès S3 Object Lambda, les API directes Amazon EBS sur les instantanés EBS, les points d'accès S3, les flux DynamoDB, les tables créées par Lake Formation, etc. AWS Glue

Pour en savoir plus sur les sélecteurs d'événements avancés, consultez Configuration des sélecteurs d'événements avancés.

Pour afficher les paramètres du sélecteur d'événements avancés pour un journal de suivi, exécutez la commande `get-event-selectors` suivante. Vous devez exécuter cette commande depuis la AWS région dans laquelle le parcours a été créé (la région d'origine) ou vous devez spécifier cette région en ajoutant le --region paramètre.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Si le sentier est un sentier organisé par une organisation et que vous êtes connecté avec un compte de membre de l'organisation en AWS Organizations, vous devez fournir l'ARN complet du sentier, et pas seulement son nom.

L'exemple suivant renvoie les paramètres par défaut pour un sélecteur d'événements avancés pour un journal de suivi. Par défaut, aucun sélecteur d'événement avancé n'est configuré pour un journal de suivi.

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour créer un sélecteur d'événements avancés, exécutez la commande `put-event-selectors`. Lorsqu'un événement lié aux données se produit dans votre compte, CloudTrail évalue la configuration de vos sentiers. Si l'événement correspond à un sélecteur d'événements avancé pour un journal de suivi, il est traité et journalisé par le journal de suivi. Vous pouvez configurer jusqu'à 500 conditions sur un journal de suivi, y compris toutes les valeurs spécifiées pour tous les sélecteurs d'événements avancés de votre journal de suivi. Pour plus d'informations, consultez Journalisation des événements de données.

Rubriques

- Exemple: journal de suivi avec sélecteurs d'événements spécifiques avancés
- Exemple de parcours utilisant des sélecteurs d'événements avancés personnalisés pour enregistrer Amazon S3 sur les événements liés aux AWS Outposts données
- Exemple de parcours utilisant des sélecteurs d'événements avancés pour exclure AWS Key Management Service des événements
- Exemple de parcours utilisant des sélecteurs d'événements avancés pour exclure les événements de gestion de l'API Amazon RDS Data

Exemple: journal de suivi avec sélecteurs d'événements spécifiques avancés

L'exemple suivant crée des sélecteurs d'événements avancés personnalisés pour un journal nommé de manière *`TrailName`*à inclure les événements de gestion de lecture et d'écriture (en

omettant le `readOnly` sélecteur) et les événements de `DeleteObject` données pour toutes les combinaisons de compartiments `PutObject` et de préfixes Amazon S3, à l'exception d'un bucket nommé `sample_bucket_name` et d'événements de données pour une fonction nommée. AWS Lambda `MyLambdaFunction` Comme il s'agit de sélecteurs d'événements avancés personnalisés, chaque ensemble de sélecteurs a un nom descriptif. Notez qu'une barre oblique de fin fait partie de la valeur ARN pour les compartiments S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

L'exemple renvoie le sélecteur d'événements avancés configuré pour le journal de suivi.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
```

```
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
```

```
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Exemple de parcours utilisant des sélecteurs d'événements avancés personnalisés pour enregistrer Amazon S3 sur les événements liés aux AWS Outposts données

L'exemple suivant montre comment configurer votre parcours pour inclure tous les événements de données relatifs à tous les Amazon S3 relatifs aux AWS Outposts objets de votre avant-poste. Dans cette version, la valeur prise en charge pour S3 sur les AWS Outposts événements du `resources.type` champ est`AWS::S3Outposts::Object`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

La commande renvoie l'exemple de résultat suivant.

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
```

```
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

Exemple de parcours utilisant des sélecteurs d'événements avancés pour exclure AWS Key Management Service des événements

L'exemple suivant crée un sélecteur d'événements avancé pour un journal nommé *TrailName*pour inclure les événements de gestion en lecture seule et en écriture seule (en omettant le `readOnly` sélecteur), mais pour exclure () les événements. AWS Key Management Service AWS KMSÉtant donné que les AWS KMS événements sont traités comme des événements de gestion et qu'ils peuvent être nombreux, ils peuvent avoir un impact important sur votre CloudTrail facture si vous disposez de plusieurs pistes qui enregistrent les événements de gestion.

Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

Pour recommencer à enregistrer AWS KMS des événements dans un journal, supprimez le `eventSource` sélecteur et réexécutez la commande.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

L'exemple renvoie le sélecteur d'événements avancés configuré pour le journal de suivi.

```
{
```

```
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour redémarrer la journalisation des événements exclus dans un journal de suivi, supprimez le sélecteur `eventSource`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Exemple de parcours utilisant des sélecteurs d'événements avancés pour exclure les événements de gestion de l'API Amazon RDS Data

L'exemple suivant crée un sélecteur d'événements avancé pour un journal nommé de manière *TrailName*à inclure les événements de gestion en lecture seule et en écriture seule (en omettant le `readOnly` sélecteur), mais pour exclure les événements de gestion de l'API Amazon RDS Data. Pour exclure les événements de gestion de l'API Amazon RDS Data, spécifiez la source de l'événement Amazon RDS Data API dans la valeur de chaîne du `eventSource` champ :. `rdsdata.amazonaws.com`

Si vous choisissez de ne pas enregistrer les événements de gestion, les événements de gestion de l'API Amazon RDS Data ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des événements de l'API Amazon RDS Data.

Pour recommencer à consigner les événements de gestion de l'API Amazon RDS Data dans un journal, supprimez le `eventSource` sélecteur et réexécutez la commande.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

L'exemple renvoie le sélecteur d'événements avancés configuré pour le journal de suivi.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour redémarrer la journalisation des événements exclus dans un journal de suivi, supprimez le sélecteur `eventSource`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Arrêt et démarrage de la journalisation pour un journal de suivi

Les commandes suivantes démarrent et arrêtent la CloudTrail journalisation.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> Avant de supprimer un compartiment, exécutez la commande `stop-logging` pour arrêter de livrer des événements au compartiment. Si vous n'arrêtez pas la journalisation, CloudTrail tente de transférer les fichiers journaux vers un bucket portant le même nom pendant une période limitée.
> Si vous arrêtez de consigner ou supprimez un parcours, CloudTrail Insights est désactivé sur ce parcours.

Suppression d'un journal de suivi

Si vous avez activé les événements CloudTrail de gestion dans Amazon Security Lake, vous devez gérer au moins un journal organisationnel multirégional qui enregistre à la fois les `read` événements de gestion et les événements `write` de gestion. Vous ne pouvez pas supprimer une piste si c'est la seule qui répond à cette exigence, sauf si vous désactivez les événements CloudTrail de gestion dans Security Lake.

Vous pouvez supprimer un journal de suivi avec la commande suivante. Vous pouvez supprimer un journal de suivi uniquement dans la région où il a été créé.

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Lorsque vous supprimez un journal de suivi, vous ne supprimez pas le compartiment Amazon S3 ni la rubrique Amazon SNS associée. Utilisez l'API AWS Management Console AWS CLI, ou service pour supprimer ces ressources séparément.

Création d'un journal de suivi pour une organisation

Si vous avez créé une organisation dans AWS Organizations, vous pouvez créer un suivi qui enregistre tous les événements pour tous les membres Comptes AWS de cette organisation. Ce journal est parfois appelé journal de suivi de l'organisation.

Le compte de gestion de l'organisation peut charger un administrateur délégué de créer des journaux de suivi d'organisation ou de gérer ceux qui existent déjà. Pour plus d'informations sur l'ajout d'un administrateur délégué, consultez Ajouter un administrateur CloudTrail délégué.

Le compte de gestion de l'organisation peut modifier un journal de suivi existant dans son compte et l'appliquer à une organisation, ce qui en fait un journal de suivi d'organisation. Les journaux de suivi de l'organisation journalisent les événements pour le compte de gestion et pour tous les comptes membres de l'organisation. Pour plus d'informations AWS Organizations, voir Terminologie et concepts des organisations.

> **Note**
>
> Vous devez vous connecter avec le compte de gestion ou le compte d'administrateur délégué associé à une organisation pour créer un journal de suivi d'organisation. Vous devez également disposer d'autorisations suffisantes pour que l'utilisateur ou le rôle du compte de gestion ou d'administrateur délégué puisse créer le journal. Si vous ne disposez pas des autorisations suffisantes, vous n'aurez pas la possibilité d'appliquer le journal de suivi à une organisation.

Tous les parcours d'organisation créés à l'aide de la console sont des journaux d'organisation multirégionaux qui enregistrent les événements associés aux comptes activés Régions AWS dans chaque compte membre de l'organisation. Pour enregistrer les événements dans toutes les AWS partitions de votre organisation, créez un journal d'organisation multirégional dans chaque partition. Vous pouvez créer un journal d'organisation à région unique ou multirégionale à l'aide du. AWS

CLI Si vous créez un sentier à région unique, vous enregistrez l'activité uniquement dans le sentier Région AWS (également appelé région d'origine).

Bien que la plupart Régions AWS soient activées par défaut pour vous Compte AWS, vous devez activer manuellement certaines régions (également appelées régions optionnelles). Pour plus d'informations sur les régions activées par défaut, consultez la section Considérations relatives à l'activation et à la désactivation des régions dans le Guide de AWS Account Management référence. Pour la liste des régions prises CloudTrail en charge, voirCloudTrail Régions prises en charge.

Lorsque vous créez un historique d'organisation, une copie du journal portant le nom que vous lui donnez est créée dans les comptes des membres appartenant à votre organisation.

- Si le parcours de l'organisation concerne une seule région et que la région d'origine du sentier n'est pas une région OPT, une copie du parcours est créée dans la région d'origine du parcours de l'organisation dans chaque compte membre.
- Si le parcours de l'organisation concerne une seule région et que la région d'origine du sentier est une région OPT, une copie du parcours est créée dans la région d'origine du parcours de l'organisation sur les comptes des membres qui ont activé cette région.
- Si le parcours de l'organisation est multirégional et que la région d'origine du sentier n'est pas une région optionnelle, une copie du parcours est créée dans chaque région activée Région AWS dans chaque compte membre. Lorsqu'un compte membre active une région optionnelle, une copie du parcours multirégional est créée dans la région nouvellement inscrite pour le compte du membre une fois l'activation de cette région terminée.
- Si le parcours de l'organisation est multirégional et que la région d'origine est une région optionnelle, les comptes membres n'enverront aucune activité au parcours de l'organisation à moins qu'ils n'aient choisi celui Région AWS où le parcours multirégional a été créé. Par exemple, si vous créez un parcours multirégional et que vous choisissez la région Europe (Espagne) comme région d'origine du parcours, seuls les comptes membres ayant activé la région Europe (Espagne) pour leur compte enverront l'activité de leur compte au parcours de l'organisation.

> **Note**
>
> CloudTrail crée des traces d'organisation dans les comptes des membres même en cas d'échec de la validation des ressources. Voici des exemples d'échecs de validation :
>
> - une politique de compartiment Amazon S3 incorrecte
> - une politique de rubrique Amazon SNS incorrecte

- impossibilité de livrer à un groupe de CloudWatch journaux Logs
- autorisation insuffisante pour chiffrer à l'aide d'une clé KMS

Un compte membre disposant d' CloudTrail autorisations peut voir les échecs de validation d'un journal d'organisation en consultant la page de détails du journal sur la CloudTrail console ou en exécutant la AWS CLI get-trail-statuscommande.

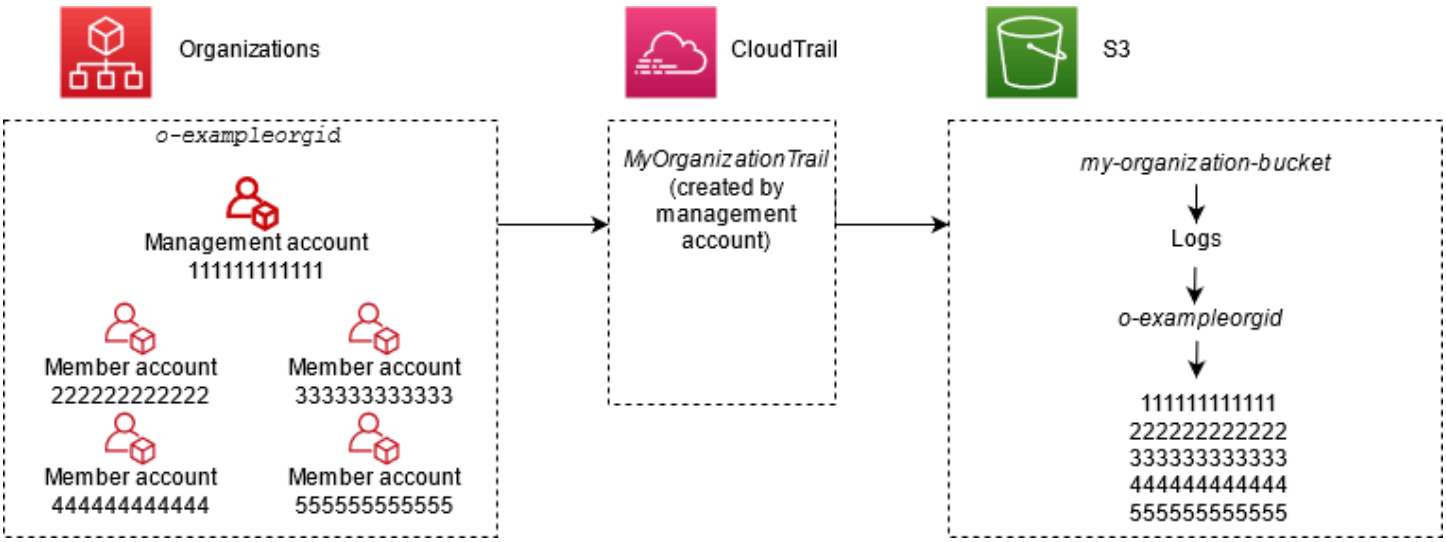
Les utilisateurs disposant CloudTrail d'autorisations sur les comptes membres peuvent consulter les traces de l'organisation lorsqu'ils se connectent à la AWS CloudTrail console depuis leur Comptes AWS compte ou lorsqu'ils exécutent AWS CLI des commandes telles que`describe-trails`. Toutefois, les utilisateurs des comptes membres ne disposent pas des autorisations suffisantes pour supprimer les traces d'une organisation, activer ou désactiver la connexion, modifier les types d'événements enregistrés ou modifier de quelque manière que ce soit le journal d'une organisation.

Lorsque vous créez un journal d'organisation dans la console, ou lorsque vous l'activez en CloudTrail tant que service fiable dans Organizations, cela crée un rôle lié au service pour effectuer des tâches de journalisation dans les comptes membres de votre organisation. Ce rôle est nommé AWSServiceRoleForCloudTrailet est requis pour CloudTrail consigner les événements d'une organisation. Si un Compte AWS est ajouté à une organisation, le suivi de l'organisation et le rôle lié au service y sont ajoutés Compte AWS, et la journalisation de ce compte démarre automatiquement dans le journal de l'organisation. Si un Compte AWS est supprimé d'une organisation, le parcours de l'organisation et le rôle lié au service sont supprimés de l'organisation Compte AWS qui ne fait plus partie de l'organisation. Toutefois, les fichiers journaux que le compte supprimé a créés avant la suppression du compte sont conservés dans le compartiment Simple Storage Service (Amazon S3) dans lequel les fichiers journaux sont stockés pour le journal de suivi.

Si le compte de gestion d'une AWS Organizations organisation crée un suivi d'organisation, puis est ensuite supprimé en tant que compte de gestion de l'organisation, tout journal d'organisation créé à l'aide de son compte devient un journal non organisationnel.

Dans l'exemple suivant, le compte de gestion 111111111111 de l'organisation crée un journal nommé MyOrganizationTrailen l'honneur de l'organisation o-exampleorgid. Le journal de suivi journalise l'activité de tous les comptes de l'organisation dans le même compartiment Amazon S3. Tous les comptes de l'organisation peuvent voir *MyOrganizationTrail*leur liste de parcours, mais les comptes membres ne peuvent pas

supprimer ou modifier le parcours de l'organisation. Seuls les comptes de gestion ou d'administrateur délégué peuvent modifier ou supprimer le journal de suivi pour l'organisation. Seul le compte de gestion peut supprimer un compte membre d'une organisation. De même, par défaut, seul le compte de gestion a accès au compartiment Amazon S3 *my-organization-bucket*pour le suivi et aux journaux qu'il contient. La structure de compartiment de haut niveau des fichiers journaux contient un dossier nommé avec l'ID de l'organisation et des sous-dossiers nommés avec l'ID de compte de chaque compte de l'organisation. Les événements de chaque compte membre sont journalisés dans le dossier qui correspond à l'ID du compte membre. Si le compte de membre 444444444444 est supprimé de l'organisation, que le rôle lié au service n'apparaît plus dans le AWS compte 444444444444, *MyOrganizationTrail*et qu'aucun autre événement n'est enregistré pour ce compte par le journal de l'organisation. Toutefois, le dossier 444444444444 demeure dans le compartiment Amazon S3, avec tous les journaux créés avant la suppression du compte de l'organisation.



Dans cet exemple, l'ARN du journal de suivi créé dans le compte de gestion est `aws:cloudtrail:us-east-2:111111111111:trail/`*`MyOrganizationTrail`*. Cet ARN est aussi l'ARN du journal de suivi de tous les comptes membres.

Les journaux de suivi d'une organisation sont similaires en de nombreux points aux journaux de suivi réguliers. Vous pouvez créer plusieurs journaux de suivi pour votre organisation et choisir de créer un journal de suivi d'organisation dans toutes les régions ou dans une seule région, ainsi que les types d'événements que vous souhaitez journaliser le journal de suivi de votre organisation, tout comme dans n'importe quel autre journal de suivi. Cependant, il existe quelques différences. Par exemple, lorsque vous créez un journal dans la console et que vous choisissez de consigner les événements de données pour les compartiments ou les AWS Lambda fonctions Amazon S3, les seules ressources répertoriées dans la CloudTrail console sont celles du compte de gestion,

mais vous pouvez ajouter les ARN pour les ressources des comptes membres. Les événements de données pour les ressources des comptes membres spécifiés sont journalisés sans avoir à configurer manuellement d'accès croisé entre comptes à ces ressources. Pour plus d'informations sur la journalisation des événements de gestion, des événements Insights et des événements liés aux donnéesJournalisation des événements de gestion, consultezJournalisation des événements de données, etJournalisation des événements Insights.

> **Note**
>
> Dans la console, vous créez un parcours multirégional. Il s'agit d'une bonne pratique recommandée ; la journalisation des activités dans toutes les régions de votre région vous Compte AWS permet de renforcer la sécurité de votre AWS environnement. Pour créer un journal de suivi à région unique, utilisez l' AWS CLI.

Lorsque vous consultez les événements dans l'historique des événements d'une organisation à laquelle vous êtes connecté AWS Organizations, vous ne pouvez consulter les événements que pour celle Compte AWS à laquelle vous êtes connecté. Par exemple, si vous êtes connecté avec le compte de gestion de l'organisation, Event history (Historique des événements) affiche les 90 derniers jours d'événements de gestion pour le compte de gestion. Les événements de compte membre de l'organisation ne sont pas affichés dans Event history (Historique des événements) pour le compte de gestion. Pour afficher les événements de compte membre dans Event history (Historique des événements), connectez-vous avec le compte membre.

Vous pouvez configurer d'autres AWS services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux d'un journal d'entreprise et agir en conséquence, de la même manière que vous le feriez pour n'importe quel autre journal. Par exemple, vous pouvez analyser les données du journal de suivi d'une organisation avec Amazon Athena. Pour plus d'informations, consultez AWS intégrations de services avec journaux CloudTrail .

Rubriques

Passer des traces des comptes membres aux traces des organisations

Si vous avez déjà configuré des CloudTrail parcours pour des comptes de membres individuels, mais que vous souhaitez passer à un suivi d'organisation afin de consigner les événements de tous les comptes, vous ne voulez pas perdre des événements en supprimant les traces de comptes de membres individuels avant de créer un suivi d'organisation. Mais lorsque vous avez deux journaux de suivi, vous vous exposez à des coûts plus élevés car des copies supplémentaires d'événements sont livrées au journal de suivi de l'organisation.

Pour vous aider à gérer les coûts tout en évitant de perdre des événements avant le début de la remise du journal aux journaux de suivi d'une organisation, nous vous conseillons de conserver à la fois les journaux de suivi de votre compte membre individuel et de votre organisation pendant une journée. Cela garantit que le journal de suivi d'une organisation journalise tous les événements, mais que les coûts d'événement dupliqués sont limités à une journée. Après le premier jour, vous pouvez arrêter de connecter (ou supprimer) les journaux de suivi des comptes membres individuels.

Se préparer pour la création d'un journal de suivi pour son organisation

Avant de créer un journal de suivi pour votre organisation, assurez-vous que le compte de gestion ou le compte d'administrateur délégué de votre organisation est correctement configuré pour la création de journaux de suivi.

- Votre organisation doit avoir toutes les fonctions activées avant de pouvoir créer un journal de suivi. Pour en savoir plus, consultez Activation de toutes les fonctions de votre organisation.
- Le compte de gestion doit avoir le rôle AWSServiceRoleForOrganizations. Ce rôle est créé automatiquement par Organizations lorsque vous créez votre organisation et est nécessaire pour CloudTrail consigner les événements d'une organisation. Pour plus d'informations, consultez Organizations et rôles liés à un service.
- Le rôle ou l'utilisateur qui crée le journal de suivi d'organisation dans le compte de gestion ou d'administrateur délégué doit disposer d'autorisations suffisantes pour créer un journal de suivi d'organisation. Vous devez au moins appliquer la politique AWSCloudTrail_FullAccess, ou une politique équivalente, à ce rôle ou à cet utilisateur. Vous devez également disposer d'autorisations suffisantes dans IAM et Organizations pour créer le rôle lié à un service et activer l'accès de confiance. Si vous choisissez de créer un nouveau compartiment S3 pour un journal organisationnel à l'aide de la CloudTrail console, votre police doit également inclure le `s3:PutEncryptionConfiguration` action car le chiffrement côté serveur est activé par défaut pour le compartiment. L'exemple de politique suivant illustre les autorisations minimales requises.

> **Note**
>
> Vous ne devez pas partager la AWSCloudTrail_FullAccesspolitique de manière générale entre vous Compte AWS. Vous devez plutôt le limiter aux Compte AWS administrateurs en raison de la nature très sensible des informations collectées par CloudTrail. Les utilisateurs ayant ce rôle ont la possibilité de désactiver ou de reconfigurer les fonctions d'audit les plus sensibles et les plus importantes dans leur Comptes AWS. C'est pourquoi vous devez contrôler et surveiller étroitement l'accès à cette politique d'accès.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

- Pour utiliser les AWS CLI ou les CloudTrail API afin de créer un suivi organisationnel, vous devez activer l'accès sécurisé pour CloudTrail dans Organizations, et vous devez créer manuellement un compartiment Amazon S3 avec une politique autorisant la journalisation d'un journal d'organisation. Pour plus d'informations, consultez Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface.
- Pour utiliser un rôle IAM existant afin d'ajouter la surveillance du suivi d'une organisation à Amazon CloudWatch Logs, vous devez modifier manuellement le rôle IAM afin d'autoriser la livraison des CloudWatch journaux des comptes membres au groupe CloudWatch des journaux du compte de gestion, comme illustré dans l'exemple suivant.

> **Note**
>
> Vous devez utiliser un rôle IAM et un groupe de CloudWatch journaux journaux qui existent dans votre propre compte. Vous ne pouvez pas utiliser un rôle IAM ou un groupe de CloudWatch journaux appartenant à un autre compte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Vous pouvez en savoir plus sur CloudTrail Amazon CloudWatch Logs inSurveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs. En outre, tenez compte des limites relatives aux CloudWatch journaux et des considérations relatives à la tarification du service avant de décider d'activer l'expérience dans le cadre d'un suivi organisationnel. Pour plus d'informations, consultez CloudWatch Logs Limits et Amazon CloudWatch Pricing.

- Pour journaliser les événements de données dans le journal de suivi de votre organisation pour des ressources spécifiques des comptes membres, rassemblez la liste des ARN (Amazon Resource Name) de chacune de ces ressources. Les ressources du compte membre ne sont pas affichées dans la CloudTrail console lorsque vous créez un suivi ; vous pouvez rechercher les ressources du compte de gestion sur lesquelles la collecte d'événements de données est prise en charge, telles que les compartiments S3. De même, si vous souhaitez ajouter des ressources membres spécifiques lors de la création ou de la mise à jour d'un journal de suivi de l'organisation au niveau de la ligne de commande, vous avez besoin des ARN de ces ressources.

> **Note**
>
> Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

Vous devriez également envisager de vérifier combien de parcours existent déjà dans le compte de gestion et dans les comptes des membres avant de créer un parcours d'organisation. CloudTrail limite le nombre de sentiers pouvant être créés dans chaque région. Il n'est pas possible de dépasser cette limite dans la région où vous créez le journal de suivi d'organisation du compte de gestion. Cependant, le journal de suivi sera créé dans les comptes membres, même si les comptes membres ont atteint la limite des journaux de suivi dans une région. Bien que le premier journal de suivi d'une région soit gratuit, des frais s'appliquent aux journaux de suivi supplémentaires. Pour réduire le coût potentiel d'un journal de suivi d'organisation, pensez à supprimer tous les journaux de suivi superflus du compte de gestion et des comptes membres. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Bonnes pratiques de sécurité dans le journal d'activité de l'organisation

Comme bonne pratique relative à la sécurité, nous vous recommandons d'ajouter la clé de condition `aws:SourceArn` des politiques de ressources (telles que celles des compartiments S3, des clés KMS ou des rubriques SNS) que vous utilisez avec un journal d'activité d'organisation. La valeur de `aws:SourceArn` est l'ARN du journal de suivi de l'organisation (ou les ARN, si vous utilisez la même

ressource pour plusieurs journaux de suivi, par exemple le même compartiment S3 pour stocker les journaux de plusieurs journaux d'activités). Cela garantit que la ressource, telle qu'un compartiment S3, n'accepte que les données associées au journal d'activité spécifique. L'ARN du journal d'activité doit utiliser l'ID de compte du compte de gestion. L'extrait de politique suivant illustre un exemple dans lequel plusieurs journaux d'activité utilisent la ressource.

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

Pour en savoir plus sur l'ajout de clés de condition à des politiques de ressources, consultez les points suivants:

- Politique relative aux compartiments Amazon S3 pour CloudTrail
- Configurer les politiques AWS KMS clés pour CloudTrail
- Politique relative aux rubriques Amazon SNS pour CloudTrail

Création d'un journal de suivi pour votre organisation dans la console

Pour créer un journal d'organisation à partir de la CloudTrail console, vous devez vous connecter à la console en tant qu'utilisateur ou en tant que rôle dans le compte de gestion ou d'administrateur délégué disposant des autorisations suffisantes. Si vous ne vous connectez pas avec le compte de gestion ou d'administrateur délégué, vous ne verrez pas l'option permettant d'appliquer un suivi à une organisation lorsque vous créez ou modifiez un journal depuis la CloudTrail console.

Vous pouvez configurer le journal de suivi d'une organisation de plusieurs façons. Par exemple, vous pouvez configurer les détails suivants pour le journal de suivi de votre organisation :

- Par défaut, lorsque vous créez un journal de suivi dans la console, le journal de suivi journalise toutes les Régions AWS de la partition AWS dans laquelle vous opérez. À titre de bonne pratique, nous vous recommandons vivement de consigner les événements dans toutes les régions de votre pays Compte AWS. Pour créer un journal de suivi pour une région unique, utilisez l' AWS CLI.
- Spécifiez s'il convient d'appliquer le journal de suivi à votre organisation. Par défaut, les journaux de suivi ne sont pas appliqués aux organisations. Vous devez choisir cette option pour créer un journal de suivi d'organisation.

- Spécifiez le compartiment Amazon S3 qui réceptionne les fichiers journaux du journal de suivi d'organisation. Vous pouvez choisir un compartiment Amazon S3 existant dans le compte de gestion, ou en créer un spécifiquement pour le journal de suivi de l'organisation.
- Pour les événements de gestion et de données, spécifiez si vous souhaitez journaliser les événements Lecture, les événements Écriture, ou les deux. CloudTrailLes événements Insights sont enregistrés uniquement sur les événements de gestion. Il est possible de spécifier la journalisation des événements de données pour des ressources présentes dans le compte de gestion en les choisissant à partir des listes de la console, et dans les comptes membres lorsque vous spécifiez l'ARN de chaque ressource pour laquelle vous souhaitez activer la journalisation des événements de données. Pour plus d'informations, consultez Événements de données.

Pour créer un parcours d'organisation à l'aide du AWS Management Console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.

   Vous devez être connecté à l'aide d'une identité IAM dans le compte de gestion ou d'administrateur délégué avec des autorisations suffisantes pour créer un journal de suivi d'organisation.
2. Choisissez Journaux de suivi, puis Créer un journal de suivi.
3. Sur la page Create Trail (Créer un journal d'activité), tapez un nom pour votre journal d'activité dans la zone Trail Name (Nom du journal d'activité). Pour plus d'informations, consultez Exigences de dénomination.
4. Sélectionnez Activer pour tous les comptes de mon organisation. Cette option ne s'affiche que si vous vous connectez à la console avec un utilisateur ou un rôle du compte de gestion ou d'administrateur délégué. Pour créer avec succès le journal de suivi d'une organisation, assurez-vous que l'utilisateur ou le rôle dispose d'autorisations suffisantes.
5. Sous Storage location (Emplacement de stockage), sélectionnez Create new S3 bucket (Créer un nouveau compartiment S3) pour créer un compartiment. Lorsque vous créez un bucket, il CloudTrail crée et applique les politiques de bucket requises.

   > **Note**
   >
   > Si vous avez choisi Utilisation du compartiment S3 existant, spécifiez un compartiment dans Nom du compartiment du journal de suivi, ou sélectionnez Parcourir pour choisir un compartiment. Vous pouvez choisir un bucket appartenant à n'importe quel compte,

mais la politique du bucket doit CloudTrail autoriser l'écriture dans ce compartiment. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.

Pour retrouver plus facilement vos journaux, créez un nouveau dossier (également appelé préfixe) dans un compartiment existant pour stocker vos CloudTrail journaux. Saisir le préfixe dans Préfixe.

6. Sous Chiffrement SSE-KMS du fichier journal, choisissez Activé si vous souhaitez chiffrer vos fichiers journaux avec SSE-KMS plutôt qu'avec SSE-S3. La valeur par défaut est Activé. Si vous n'activez pas le chiffrement SSE-KMS, vos journaux sont chiffrés à l'aide du chiffrement SSE-S3. Pour plus d'informations sur le chiffrement SSE-KMS, consultez Utilisation du chiffrement côté serveur avec AWS Key Management Service (SSE-KMS). Pour plus d'informations sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3).

   Si vous activez le chiffrement SSE-KMS, sélectionnez Nouveau ou Existant. AWS KMS key Dans AWS KMS Alias, spécifiez un alias au format `alias/` *`MyAliasName`*. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS.

   > **Note**
   >
   > Vous pouvez également saisir l'ARN d'une clé à partir d'un autre compte. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS. La politique de clé doit CloudTrail autoriser l'utilisation de la clé pour chiffrer vos fichiers journaux et permettre aux utilisateurs que vous spécifiez de lire les fichiers journaux sous forme non chiffrée. Pour en savoir plus sur la modification manuelle de la politique de clés, consultez Configurer les politiques AWS KMS clés pour CloudTrail.

7. Sous Paramètres supplémentaires, configurez les événements suivants.

   a. Sous Validation du fichier journal, choisissez Activé pour que les fichiers de valeur de hachage soient livrés dans votre compartiment S3. Vous pouvez utiliser les fichiers de synthèse pour vérifier que vos fichiers journaux n'ont pas changé après leur CloudTrail livraison. Pour plus d'informations, consultez Validation de l' CloudTrail intégrité du fichier journal.

b. Pour l'envoi de notifications SNS, choisissez Enabled pour être averti chaque fois qu'un journal est envoyé à votre bucket. CloudTrail enregistre plusieurs événements dans un fichier journal. Des notifications SNS sont envoyées pour chaque fichier journal, non pour chaque événement. Pour plus d'informations, consultez Configuration des notifications Amazon SNS pour CloudTrail.

   Si vous activez les notifications SNS, pour Créer une nouvelle rubrique SNS, choisissez Nouveau pour créer une rubrique, ou Existant, pour utiliser une rubrique existante. Si vous créez un journal de suivi qui s'applique à toutes les régions, les notifications SNS relatives à la livraison de fichiers journaux de toutes les régions sont envoyées à la rubrique SNS unique que vous créez.

   Si vous choisissez Nouveau, vous CloudTrail spécifiez le nom du nouveau sujet ou vous pouvez saisir un nom. Si vous choisissez Existant, choisissez une rubrique SNS dans la liste déroulante. Vous pouvez également saisir l'ARN d'une rubrique provenant d'une autre région ou d'un compte disposant des autorisations appropriées. Pour plus d'informations, consultez Politique relative aux rubriques Amazon SNS pour CloudTrail.

   Si vous créez une rubrique, vous devez vous abonner à la rubrique pour être averti de l'envoi de fichiers journaux. Vous pouvez vous abonner à partir de la console Amazon SNS. En raison de la fréquence des notifications, nous vous recommandons de configurer l'abonnement pour pouvoir utiliser une file d'attente Amazon SQS afin de gérer les notifications par programmation. Pour plus d'informations, consultez Prise en main d'Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

8. Vous pouvez éventuellement configurer CloudTrail pour envoyer des fichiers CloudWatch journaux à Logs en choisissant Enabled in CloudWatch Logs. Pour plus d'informations, consultez Envoyer des événements à CloudWatch Logs.

> **Note**
>
> Seul le compte de gestion peut configurer un groupe de CloudWatch journaux pour un journal d'entreprise à l'aide de la console. L'administrateur délégué peut configurer un groupe de CloudWatch journaux Logs à l'aide des opérations AWS CLI CloudTrail `CreateTrail` ou de `UpdateTrail` l'API.

a. Si vous activez l'intégration aux CloudWatch journaux, choisissez Nouveau pour créer un nouveau groupe de journaux ou Existant pour utiliser un groupe existant. Si vous choisissez Nouveau, vous CloudTrail spécifiez un nom pour le nouveau groupe de journaux ou vous pouvez saisir un nom.

b. Si vous choisissez Existant, choisissez un groupe de journaux dans la liste déroulante.

c. Choisissez Nouveau pour créer un nouveau rôle IAM afin d'obtenir les autorisations d'envoyer des CloudWatch journaux à Logs. Choisir Existant pour choisir un rôle IAM existant dans la liste déroulante. L'instruction de politique pour le rôle nouveau ou existant s'affiche lorsque vous déroulez Document de politique. Pour plus d'informations sur ce rôle, consultez Document de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance.

> **Note**
>
> Lorsque vous configurez un journal de suivi, vous pouvez choisir un compartiment S3 et une rubrique Amazon SNS qui appartiennent à un autre compte. Toutefois, si vous souhaitez CloudTrail transmettre des événements à un groupe de CloudWatch journaux journaux, vous devez choisir un groupe de journaux existant dans votre compte actuel.

9. Pour Balises, ajoutez une ou plusieurs identifications personnalisées (paires clé-valeur) à votre journal de suivi. Les balises peuvent vous aider à identifier à la fois vos CloudTrail traces et les compartiments Amazon S3 contenant les fichiers CloudTrail journaux. Vous pouvez ensuite utiliser des groupes de ressources pour vos CloudTrail ressources. Pour plus d'informations, consultez AWS Resource Groups et Balises.

10. Sur la page Choisir des événements du journal, choisissez les types d'événements que vous souhaitez consigner. Sous Événements de gestion, procédez comme suit.

    a. Pour Activité d'API, indiquez si vous souhaitez que votre journal de suivi journalise les événements en événements Lecture ou en événements Écriture, ou les deux. Pour plus d'informations, consultez Événements de gestion.

    b. Choisissez Exclure les AWS KMS événements pour filtrer AWS Key Management Service (AWS KMS) les événements de votre parcours. Le paramètre par défaut est d'inclure tous les événements AWS KMS .

L'option permettant d'enregistrer ou d'exclure AWS KMS des événements n'est disponible que si vous enregistrez des événements de gestion sur votre parcours. Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

AWS KMS des actions telles que `EncryptDecrypt`, et génèrent `GenerateDataKey` généralement un grand volume (plus de 99 %) d'événements. Ces actions sont désormais journalisées en tant qu'événements Lecture. Les AWS KMS actions pertinentes à faible volume telles que `DisableDelete`, et `ScheduleKey` (qui représentent généralement moins de 0,5 % du volume d' AWS KMS événements) sont enregistrées en tant qu'événements d'écriture.

Pour exclure les événements de volume important tels que `Encrypt`, `Decrypt` et `GenerateDataKey`, tout en continuant de journaliser les événements pertinents tels que `Disable`, `Delete` et `ScheduleKey`, choisissez de journaliser les événements de gestion Écriture et effacez la case à cocher pour Exclure les événements AWS KMS .

c. Choisissez Exclure les événements API de données Amazon RDS pour filtrer les événements d'API de données Amazon Relational Database Service Data hors de votre journal de suivi. Le paramètre par défaut consiste à inclure tous les événements d'API de données Amazon RDS. Pour plus d'informations sur les événements d'API Amazon RDS Data API, consultez Journalisation des appels d'API de données avec AWS CloudTrail dans le Guide de l'utilisateur Amazon RDS pour Aurora.

11. Pour journaliser les événements de données, choisissez Événements de données. Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour plus d'informations, consultez Tarification AWS CloudTrail.

12. **Important**

    Les étapes 12 à 16 concernent la configuration des événements de données à l'aide de sélecteurs d'événements avancés, ce qui est le cas par défaut. Les sélecteurs d'événements avancés vous permettent de configurer davantage de types d'événements de données et de contrôler avec précision les événements de données capturés par votre journal de suivi. Si vous avez choisi d'utiliser des sélecteurs d'événements de base, suivez les étapes décrites dans Configurer les paramètres des événements de

données à l'aide de sélecteurs d'événements de base, puis revenez à l'étape 17 de cette procédure.

Pour Type d'événement de données, choisissez le type de ressource sur lequel vous souhaitez journaliser les événements de données. Pour plus d'informations sur les types d'événements de données, veuillez consulter Événements de données.

> **Note**
>
> Pour enregistrer les événements de données pour AWS Glue les tables créées par Lake Formation, choisissez Lake Formation.

13. Choisissez un modèle de sélecteur de journaux. CloudTrail inclut des modèles prédéfinis qui enregistrent tous les événements de données pour le type de ressource. Pour créer un modèle de sélecteur de journal personnalisé, choisissez Personnaliser.

> **Note**
>
> Le choix d'un modèle prédéfini pour les compartiments S3 permet de consigner les événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois le suivi terminé. Il permet également de consigner l'activité des événements de données effectuée par n'importe quelle identité IAM de votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
> Si le journal de suivi s'applique à une seule région, le fait de choisir un modèle prédéfini qui journalise tous les compartiments S3 permet la journalisation des événements de données pour tous les compartiments situés dans la même région que votre journal de suivi et tous les compartiments que vous créerez ultérieurement dans cette région. Il ne va pas journaliser les d'événements de données pour les compartiments Amazon S3 situés dans d'autres régions de votre compte AWS .
> Si vous créez un suivi pour toutes les régions, le choix d'un modèle prédéfini pour les fonctions Lambda permet de consigner les événements de données pour toutes les fonctions actuellement présentes dans votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans n'importe quelle région une fois le suivi créé. Si vous créez un suivi pour une seule région (en utilisant le AWS CLI), cette sélection active l'enregistrement des événements de données pour toutes les fonctions

actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une fois que vous aurez fini de créer le journal. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions.
La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectuée par n'importe quelle identité IAM de votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

14. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.
15. Dans Sélecteurs d'événements avancés, créez une expression pour les ressources spécifiques sur lesquelles vous souhaitez journaliser les événements de données. Vous pouvez ignorer cette étape si vous utilisez un modèle de journal prédéfini.

    a. Choisissez parmi les options suivantes.

    - **`readOnly`**- `readOnly` peut être défini pour être égal à une valeur de `true` ou`false`. Les événements de données en lecture seule sont des événements qui ne modifient pas l'état d'une ressource, tels que les événements `Get*` ou `Describe*`. Les événements d'écriture ajoutent, modifient ou suppriment des ressources, des attributs ou des artefacts, tels que les événements `Put*`, `Delete*`, ou `Write*`. Pour journaliser les deux événements `read` et `write`, n'ajoutez pas de sélecteur `readOnly`.
    - **`eventName`** - `eventName` peut utiliser n'importe quel opérateur. Vous pouvez l'utiliser pour inclure ou exclure tout événement de données enregistré CloudTrail, tel que `PutBucketPutItem`, ou`GetSnapshotBlock`.
    - **`resources.ARN`**- Vous pouvez utiliser n'importe quel opérateur`resources.ARN`, mais si vous utilisez égal ou non, la valeur doit correspondre exactement à l'ARN d'une ressource valide du type que vous avez spécifié dans le modèle comme valeur de`resources.type`.

      Le tableau suivant affiche le format ARN valide de chaque `resources.type`.

> **Note**
>
> Vous ne pouvez pas utiliser le `resources.ARN` champ pour filtrer les types de ressources dépourvus d'ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name /` `arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`
`AWS::Bedrock::AgentAlias`	`arn:partition :bedrock: region:account_ID :agent-alias/ agent_ID/alias_ID`
`AWS::Bedrock::KnowledgeBase`	`arn:partition :bedrock: region:account_ID :knowledge-base/knowledge_base_ID`

resources.type	resources.ARN
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*

resources.type	resources.ARN
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*

resources.type	resources.ARN
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*

resources.type	resources.ARN
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*

resources.type	resources.ARN
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemake r: *region*:*account_ID* :feature- group/ *feature_group_name*

resources.type	resources.ARN
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Pour les tables ayant les flux activés, le champ `resources` dans l'événement de plan de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.

[2] Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante. La barre oblique de fin est intentionnelle ; ne l'excluez pas.

[3] Pour journaliser les événements sur tous les objets d'un point d'accès S3, il est recommandé d'utiliser uniquement l'ARN du point d'accès, de ne pas inclure le chemin d'accès de l'objet et d'utiliser les opérateurs `StartsWith` ou `NotStartsWith`.

Pour plus d'informations sur les formats ARN des ressources d'événements de données, consultez Actions, ressources et clés de condition dans le Guide de l'utilisateur AWS Identity and Access Management .

b. Pour chaque champ, choisissez + Conditions pour ajouter autant de conditions que vous le souhaitez, jusqu'à un maximum de 500 valeurs spécifiées pour toutes les conditions. Par exemple, pour exclure les événements de données de deux compartiments S3 des événements de données enregistrés sur votre parcours, vous pouvez définir le champ sur Resources.ARN, définir l'opérateur pour ne commence pas par, puis coller l'ARN d'un compartiment S3 ou rechercher les compartiments S3 pour lesquels vous ne souhaitez pas enregistrer d'événements.

   Pour ajouter le deuxième compartiment S3, choisissez + Conditions, puis répétez l'instruction précédente, en collant dans l'ARN ou en recherchant un compartiment différent.

   > **Note**
   >
   > Il est possible de définir un maximum de 500 valeurs pour tous les sélecteurs d'un journal de suivi. Cela inclut des tableaux de valeurs multiples pour un sélecteur tel que `eventName`. Si vous avez défini des valeurs uniques pour tous les sélecteurs, il est possible d'ajouter un maximum de 500 conditions à un sélecteur.

Si votre compte compte compte plus de 15 000 fonctions Lambda, vous ne pouvez pas afficher ou sélectionner toutes les fonctions dans la CloudTrail console lors de la création d'un journal. Il est toujours possible de journaliser toutes les fonctions à l'aide d'un modèle de sélecteur prédéfini, même si ces dernières ne sont pas affichées. Si vous souhaitez journaliser les événements de données de fonctions spécifiques, vous pouvez ajouter manuellement une fonction si vous connaissez son ARN. Vous pouvez également terminer la création du journal dans la console, puis utiliser la put-event-selectors commande AWS CLI et pour configurer la journalisation des événements de données pour des fonctions Lambda spécifiques. Pour plus d'informations, consultez Gérer les sentiers à l'aide du AWS CLI.

c. Choisir + champ pour ajouter des champs supplémentaires au besoin. Pour éviter les erreurs, il convient de ne pas définir de valeurs conflictuelles ou en double pour les champs. Par exemple, ne spécifiez pas un ARN dans un sélecteur pour être égal à une valeur, puis spécifiez que l'ARN n'est pas égal à la même valeur dans un autre sélecteur.

16. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Ajouter un type d'événement de données. Répétez les étapes 12 à cette étape pour configurer les sélecteurs d'événements avancés pour le type d'événement de données.

17. Choisissez Insights events si vous souhaitez que votre parcours enregistre les événements CloudTrail Insights.

    Dans Type d'événement, sélectionnez Événements Insights. Dans Événements Insights, choisissez Taux d'appels d'API,Taux d'erreurs d'API, ou les deux. Vous devez journaliser les événements de gestion Écriture pour journaliser les événements Insights afin de connaître le Taux d'appels d'API. Vous devez journaliser les événements de gestion Lecture ou Écriture pour journaliser les événements Insights afin de connaître le Taux d'erreur de l'API.

    CloudTrail Insights analyse les événements de gestion pour détecter toute activité inhabituelle et enregistre les événements lorsque des anomalies sont détectées. Par défaut, les journaux de suivi ne journalisent pas les événements Insights. Pour plus d'informations sur les événements Insights, consultez Journalisation des événements Insights. Des frais supplémentaires s'appliquent pour la journalisation des événements Insights. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

    Les événements Insights sont transmis à un dossier différent nommé `/CloudTrail-Insight` dans le même compartiment S3 spécifié dans la zone Emplacement de stockage de la page de détails du journal. CloudTrailcrée le nouveau préfixe pour vous. Par exemple, si votre

compartiment S3 de destination actuel se nomme `S3bucketName/AWSLogs/CloudTrail/`, le nom du compartiment S3 avec un nouveau préfixe se nommera `S3bucketName/AWSLogs/CloudTrail-Insight/`.

18. Après avoir sélectionné les types d'événements à journaliser, choisissez Suivant.
19. Sur la page Vérifier et créer, vérifiez vos choix. Choisissez Modifier dans une section pour modifier les paramètres de journal de suivi affichés dans cette section. Lorsque vous êtes prêt à créer votre journal de suivi, choisissez Créer un journal de suivi.
20. Le nouveau journal de suivi s'affiche sur la page Trails (Journaux de suivi). Un journal de suivi d'organisation peut prendre jusqu'à 24 heures pour être créé dans toutes les régions de tous les comptes membres. La page Journaux de suivi affiche les journaux de suivi de votre compte pour toutes les Régions. En 5 minutes environ, CloudTrail publie des fichiers journaux qui indiquent les appels AWS d'API effectués dans votre organisation. Il est possible de voir les fichiers journaux se trouvent dans le compartiment Amazon S3 que vous avez spécifiés.

> **Note**
>
> Vous ne pouvez pas renommer un journal de suivi une fois qu'il a été créé. Au lieu de cela, vous pouvez supprimer le journal de suivi et en créer un nouveau.

Étapes suivantes

Après avoir créé le journal de suivi, vous pouvez le modifier :

- Modifiez la configuration de votre journal de suivi. Pour plus d'informations, consultez Mise à jour d'un journal de suivi.
- Si nécessaire, configurez le compartiment Amazon S3 pour autoriser des utilisateurs spécifiques des comptes membres à lire les fichiers journaux de l'organisation. Pour plus d'informations, consultez Partage de fichiers CloudTrail journaux entre AWS comptes.
- Configurez CloudTrail pour envoyer des fichiers journaux à CloudWatch Logs. Pour plus d'informations, reportez-vous à la section Envoyer des événements à CloudWatch Logs et à l'élément CloudWatch Logs inSe préparer pour la création d'un journal de suivi pour son organisation.

> **Note**
>
> Seul le compte de gestion peut configurer un groupe de CloudWatch journaux journaux pour le journal d'une organisation.

- Créez une table et utilisez-la pour exécuter une requête dans Amazon Athena afin d'analyser l'activité de vos services AWS . Pour plus d'informations, consultez la section Création d'une table pour les CloudTrail journaux dans la CloudTrail console dans le guide de l'utilisateur d'Amazon Athena.
- Ajoutez des identifications personnalisées (paires clé-valeur) pour le journal de suivi.
- Pour créer un autre journal de suivi d'organisation, revenez à la page Trails (Journaux de suivi) et choisissez Create trail (Créer un journal de suivi).

> **Note**
>
> Lorsque vous configurez un journal de suivi, vous pouvez choisir un compartiment Amazon S3 et une rubrique SNS qui appartiennent à un autre compte. Toutefois, si vous souhaitez CloudTrail transmettre des événements à un groupe de CloudWatch journaux journaux, vous devez choisir un groupe de journaux existant dans votre compte actuel.

Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface

Vous pouvez créer un journal de suivi d'organisation avec la AWS CLI. AWS CLI Il est régulièrement mis à jour avec des fonctionnalités et des commandes supplémentaires. Pour garantir le succès, assurez-vous d'avoir installé ou mis à jour une AWS CLI version récente avant de commencer.

> **Note**
>
> Les exemples de cette section sont spécifiques à la création et la mise à jour des journaux de suivi de l'organisation. Pour des exemples d'utilisation du AWS CLI pour gérer les sentiers, voir Gérer les sentiers à l'aide du AWS CLI etConfiguration de la surveillance des CloudWatch journaux avec le AWS CLI. Lorsque vous créez ou mettez à jour le journal d'une organisation à l'aide du AWS CLI, vous devez utiliser un AWS CLI profil du compte de gestion ou du compte d'administrateur délégué doté des autorisations suffisantes. Si

vous convertissez un journal de suivi d'organisation en un journal de suivi non lié à une organisation, vous devez utiliser le compte de gestion de l'organisation.
Vous devez configurer le compartiment Amazon S3 utilisé pour le journal de suivi d'une organisation avec des autorisations suffisantes.

Créez ou mettez à jour un compartiment Amazon S3 pour stocker les fichiers journaux du journal de suivi d'une organisation

Vous devez spécifier un compartiment Amazon S3 pour recevoir les fichiers journaux pour un journal d'activité d'une organisation. Ce compartiment doit disposer d'une politique CloudTrail permettant d'y placer les fichiers journaux de l'organisation.

Voici un exemple de politique pour un compartiment Amazon S3 nommé *myOrganizationBucket*, qui appartient au compte de gestion de l'organisation. Remplacez *myOrganizationBucket*, *region*, *ManagementAccountID*, *TrailName* et *O-OrganizationID par les valeurs de votre organisation*

Cette politique de compartiment contient trois instructions.

- La première instruction permet CloudTrail d'appeler l'`GetBucketAcl`action Amazon S3 sur le compartiment Amazon S3.
- La seconde instruction permet de se connecter dans le cas où le suivi est modifié d'un suivi d'organisation à un suivi pour ce compte uniquement.
- La troisième instruction autorise la journalisation pour le suivi d'organisation.

L'exemple de politique inclut une clé de condition `aws:SourceArn` de la politique de compartiment Amazon S3. La clé de condition globale IAM `aws:SourceArn` permet de garantir que les CloudTrail écritures dans le compartiment S3 ne concernent qu'un ou plusieurs sentiers spécifiques. Dans un journal de suivi de l'organisation, la valeur de `aws:SourceArn` doit être un ARN de suivi appartenant au compte de gestion qui utilise l'ID du compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
```

```
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Cet exemple de politique n'autorise pas tous les utilisateurs des comptes membres à accéder aux fichiers journaux créés pour l'organisation. Par défaut, les fichiers journaux de l'organisation sont accessibles uniquement au compte de gestion. Pour plus d'informations sur la manière d'autoriser un accès en lecture au compartiment Amazon S3 pour les utilisateurs IAM des comptes membres, consultez Partage de fichiers CloudTrail journaux entre AWS comptes.

Activation CloudTrail en tant que service fiable dans AWS Organizations

Avant de créer un journal de suivi d'organisation, vous devez au préalable activer toutes les fonctions dans Organizations. Pour plus d'informations, consultez Enabling All Features in Your Organization (Activation de toutes les fonctions de votre organisation) ou exécutez la commande suivante à l'aide d'un profil bénéficiant des autorisations suffisantes dans le compte de gestion :

```
aws organizations enable-all-features
```

Après avoir activé toutes les fonctionnalités, vous devez configurer Organizations pour CloudTrail qu'elles soient considérées comme des services fiables.

Pour créer une relation de service fiable entre AWS Organizations et CloudTrail, ouvrez un terminal ou une ligne de commande et utilisez un profil dans le compte de gestion. Exécutez la commande `aws organizations enable-aws-service-access` comme illustré dans l'exemple suivant.

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

Utilisation de create-trail

Créer un journal de suivi d'organisation qui s'applique à toutes les régions

Pour créer un journal de suivi d'organisation qui s'applique à toutes les régions, ajoutez les options `--is-organization-trail` et `--is-multi-region-trail`.

> **Note**
>
> Lorsque vous créez un journal d'organisation avec le AWS CLI, vous devez utiliser un AWS CLI profil du compte de gestion ou du compte d'administrateur délégué doté des autorisations suffisantes.

L'exemple suivant crée un journal de suivi d'organisation qui livre les journaux de toutes les régions à un compartiment existant nommé *my-bucket* :

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail --is-multi-region-trail
```

Afin de confirmer que votre journal de suivi existe dans toutes les régions, les paramètres `IsOrganizationTrail` et `IsMultiRegionTrail` de la sortie sont tous deux définis sur `true` :

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Exécutez la commande `start-logging` pour démarrer la journalisation pour votre journal de suivi. Pour plus d'informations, consultez Arrêt et démarrage de la journalisation pour un journal de suivi.

Créer un journal de suivi d'organisation comme journal de suivi à région unique

La commande suivante crée un journal d'organisation qui enregistre uniquement les événements dans un seul journal Région AWS, également appelé journal d'une seule région. La AWS région dans laquelle les événements sont enregistrés est la région spécifiée dans le profil de configuration du AWS CLI.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail
```

Pour plus d'informations, consultez Exigences de dénomination.

Exemple de sortie :

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

Par défaut, la commande `create-trail` crée un journal de suivi à région unique et ce suivi n'active pas la validation de fichiers journaux.

> **Note**
>
> Utilisez la commande `start-logging` pour démarrer la journalisation pour votre journal de suivi.

Exécution de update-trail pour effectuer la mise à jour d'un journal de suivi d'organisation

Vous pouvez utiliser la commande `update-trail` pour modifier les paramètres de configuration d'un journal de suivi d'organisation ou pour appliquer un journal de suivi existant d'un compte AWS à l'intégralité d'une organisation. Souvenez-vous qu'il est possible d'exécuter la commande `update-trail` qu'à partir de la région dans laquelle le journal de suivi a été créé.

> **Note**
>
> Si vous utilisez le AWS CLI ou l'un des AWS SDK pour mettre à jour un parcours, assurez-vous que la politique relative aux compartiments du parcours le soit up-to-date. Pour plus d'informations, consultez Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface.

Lorsque vous mettez à jour le journal d'une organisation avec le AWS CLI, vous devez utiliser un AWS CLI profil du compte de gestion ou du compte d'administrateur délégué doté des autorisations suffisantes. Si vous souhaitez convertir un journal d'organisation en un journal non lié à une organisation, vous devez utiliser le compte de gestion de l'organisation, car le compte de gestion est le propriétaire de toutes les ressources de l'organisation.
CloudTrail met à jour les traces de l'organisation dans les comptes des membres même en cas d'échec de la validation des ressources. Voici des exemples d'échecs de validation :

- une politique de compartiment Amazon S3 incorrecte
- une politique de rubrique Amazon SNS incorrecte
- impossibilité de livrer à un groupe de CloudWatch journaux Logs
- autorisation insuffisante pour chiffrer à l'aide d'une clé KMS

Un compte membre disposant d' CloudTrail autorisations peut voir les échecs de validation d'un journal d'organisation en consultant la page de détails du journal sur la CloudTrail console ou en exécutant la AWS CLI get-trail-statuscommande.

Application d'un journal de suivi existant à une organisation

Pour modifier un historique existant afin qu'il s'applique également à une organisation plutôt qu'à un seul AWS compte, ajoutez l'`--is-organization-trail`option, comme indiqué dans l'exemple suivant.

> **Note**
>
> Utilisez le compte de gestion pour transformer un journal de suivi non lié à une organisation existant en un journal d'organisation.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

Afin de confirmer que le journal de suivi s'applique maintenant à l'organisation, le paramètre `IsOrganizationTrail` de la sortie affiche une valeur de `true`.

```
{
    "IncludeGlobalServiceEvents": true,
```

```
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

Dans l'exemple précédent, le journal de suivi a été configuré pour s'appliquer à toutes les régions (`"IsMultiRegionTrail": true`). Un journal de suivi qui s'appliquait uniquement à une région unique indiquerait `"IsMultiRegionTrail": false` au niveau de la sortie.

Convertir un journal de suivi d'organisation qui s'applique à une région unique de sorte qu'il s'applique à toutes les régions

Pour modifier un journal de suivi d'organisation existant afin que celui-ci s'applique à toutes les régions, ajoutez l'option `--is-multi-region-trail` comme indiqué dans l'exemple suivant.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Afin de confirmer que le journal de suivi s'applique maintenant à toutes les régions, le paramètre `IsMultiRegionTrail` dans le résultat affiche une valeur de `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

Résolution des problèmes

Cette section fournit des informations sur la manière de résoudre les problèmes liés à un suivi organisationnel.

Rubriques

- CloudTrail n'organise pas d'événements

- CloudTrail n'envoie pas de notifications Amazon SNS pour le compte d'un membre d'une organisation

CloudTrail n'organise pas d'événements

Si CloudTrail les fichiers CloudTrail journaux ne sont pas envoyés au compartiment Amazon S3

Vérifiez s'il y a un problème avec le compartiment S3.

- Depuis la CloudTrail console, consultez la page de détails du parcours. En cas de problème avec le compartiment S3, la page de détails inclut un avertissement indiquant que la livraison au compartiment S3 a échoué.
- À partir du AWS CLI, exécutez la get-trail-statuscommande. En cas d'échec, la sortie de commande inclut le `LatestDeliveryError` champ, qui affiche toute erreur Amazon S3 CloudTrail rencontrée lors de la tentative de transfert de fichiers journaux vers le compartiment désigné. Cette erreur se produit uniquement en cas de problème avec le compartiment S3 de destination et ne se produit pas pour les demandes dont le délai d'expiration est dépassé. Pour résoudre le problème, corrigez la politique du compartiment afin de CloudTrail pouvoir écrire dans le compartiment ; ou créez un nouveau compartiment, puis appelez `update-trail` pour spécifier le nouveau compartiment. Pour plus d'informations sur la politique de compartiment de l'organisation, consultez Créer ou mettre à jour un compartiment Amazon S3 à utiliser pour stocker les fichiers journaux d'un journal d'organisation.

Si les journaux CloudTrail ne sont pas envoyés à CloudWatch Logs

Vérifiez s'il existe un problème avec la configuration de la politique de rôle CloudWatch Logs.

- Depuis la CloudTrail console, consultez la page de détails du parcours. En cas de problème avec CloudWatch les journaux, la page de détails inclut un avertissement indiquant que la livraison CloudWatch des journaux a échoué.
- À partir du AWS CLI, exécutez la get-trail-statuscommande. En cas d'échec, le résultat de la commande inclut le `LatestCloudWatchLogsDeliveryError` champ, qui affiche toute erreur de CloudWatch journalisation CloudTrail rencontrée lors de la tentative de transfert de CloudWatch journaux à Logs. Pour résoudre le problème, corrigez la politique relative au rôle CloudWatch des journaux. Pour plus d'informations sur la politique relative au rôle des CloudWatch journaux, consultezDocument de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance.

Si vous ne voyez aucune activité liée à un compte membre dans le journal d'une organisation

Si vous ne constatez aucune activité liée à un compte membre dans le journal d'une organisation, vérifiez les points suivants :

- Vérifiez la région d'origine du sentier pour voir s'il s'agit d'une région optionnelle

  Bien que la plupart Régions AWS soient activées par défaut pour vous Compte AWS, vous devez activer manuellement certaines régions (également appelées régions optionnelles). Pour plus d'informations sur les régions activées par défaut, consultez la section Considérations relatives à l'activation et à la désactivation des régions dans le Guide de AWS Account Management référence. Pour la liste des régions prises CloudTrail en charge, voirCloudTrail Régions prises en charge.

  Si le parcours de l'organisation est multirégional et que la région d'origine est une région optionnelle, les comptes membres n'enverront aucune activité au parcours de l'organisation à moins qu'ils n'aient choisi celui Région AWS où le parcours multirégional a été créé. Par exemple, si vous créez un parcours multirégional et que vous choisissez la région Europe (Espagne) comme région d'origine du parcours, seuls les comptes membres ayant activé la région Europe (Espagne) pour leur compte enverront l'activité de leur compte au parcours de l'organisation. Pour résoudre le problème, activez la région opt-in dans chaque compte membre de votre organisation. Pour plus d'informations sur l'activation d'une région optionnelle, voir Activer ou désactiver une région dans votre organisation dans le Guide de AWS Account Management référence.
- Vérifiez si la politique basée sur les ressources de l'organisation est en conflit avec la politique des rôles liés au CloudTrail service

  CloudTrail utilise le rôle lié au service nommé `AWSServiceRoleForCloudTrail`pour prendre en charge les traces de l'organisation. Ce rôle lié à un service permet d' CloudTrail effectuer des actions sur les ressources de l'organisation, telles que. `organizations:DescribeOrganization` Si la politique basée sur les ressources de l'organisation refuse une action autorisée dans la politique des rôles liés au service, elle ne CloudTrail pourra pas exécuter l'action même si elle est autorisée dans la politique des rôles liés au service. Pour résoudre le problème, corrigez la politique basée sur les ressources de l'organisation afin qu'elle ne refuse pas les actions autorisées dans la politique des rôles liés aux services.

CloudTrail n'envoie pas de notifications Amazon SNS pour le compte d'un membre d'une organisation

Lorsqu'un compte membre associé à un historique d' AWS Organizations organisation n'envoie pas de notifications Amazon SNS, il se peut que la configuration de la politique relative aux rubriques SNS pose problème. CloudTrail crée des traces d'organisation dans les comptes des membres même si la validation d'une ressource échoue. Par exemple, la rubrique SNS du journal de l'organisation n'inclut pas tous les identifiants de compte des membres. Si la politique des rubriques SNS est incorrecte, un échec d'autorisation se produit.

Pour vérifier si la politique des rubriques SNS d'un parcours présente un échec d'autorisation, procédez comme suit :

- Depuis la CloudTrail console, consultez la page de détails du parcours. En cas d'échec de l'autorisation, la page de détails inclut un avertissement `SNS authorization failed` et indique de corriger la politique relative aux sujets SNS.
- À partir du AWS CLI, exécutez la get-trail-statuscommande. En cas d'échec de l'autorisation, la sortie de commande inclut le `LastNotificationError` champ avec une valeur de`AuthorizationError`. Pour résoudre le problème, corrigez la politique relative aux rubriques Amazon SNS. Pour plus d'informations sur la politique relative aux rubriques Amazon SNS, consultez. Politique relative aux rubriques Amazon SNS pour CloudTrail

Pour plus d'informations sur les sujets liés aux réseaux sociaux et sur l'abonnement à ces derniers, consultez Getting started with Amazon SNS dans le manuel du développeur Amazon Simple Notification Service.

Affichage CloudTrail des événements Insights pour les sentiers

Après avoir activé CloudTrail Insights on a trail, vous pouvez consulter jusqu'à 90 jours d'événements Insights à l'aide de la CloudTrail console ou du AWS CLI. Cette section décrit comment afficher, rechercher et télécharger un fichier d'événements Insights. Pour plus d'informations sur l'utilisation de l'`LookupEvents`API pour récupérer des informations à partir d' CloudTrail événements, consultez la référence de l'AWS CloudTrail API. Pour plus d'informations sur CloudTrail Insights, consultez Journalisation des événements Insights ce guide.

Pour en savoir plus sur la création et la gestion d'un journal d'activité, consultez Création d'un journal de suivi et Obtenir et consulter vos fichiers CloudTrail journaux.

> **Note**
>
> Pour enregistrer les événements Insights sur le volume d'appels des API, le journal doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, le journal de suivi doit enregistrer les événements de gestion `read` ou `write`.

Rubriques

Afficher CloudTrail les événements Insights relatifs aux parcours dans la CloudTrail console

Une fois que vous avez activé les événements CloudTrail Insights sur un trail, lorsque vous CloudTrail détectez une activité inhabituelle d'API ou de taux d'erreur, CloudTrail génère des événements Insights et les affiche sur les pages Tableau de bord et Insights du AWS Management Console. Vous pouvez afficher les événements Insights dans la console et résoudre les problèmes liés à l'activité inhabituelle. Les événements Insights des 90 derniers jours sont affichés dans la console. Vous pouvez également télécharger les événements Insights à l'aide de la AWS CloudTrail console. Vous pouvez rechercher des événements par programmation à l'aide des AWS SDK ou. AWS Command Line Interface Pour plus d'informations sur CloudTrail les événements Insights, consultez Journalisation des événements Insights ce guide.

> **Note**
>
> Pour enregistrer les événements Insights sur le volume d'appels des API, le journal doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, le journal de suivi doit enregistrer les événements de gestion `read` ou `write`.

Une fois les événements Insights journalisés, les événements sont affichés sur la page Insights pendant 90 jours. Vous ne pouvez pas supprimer manuellement des événements de la page Insights. Étant donné que vous devez créer un suivi avant de pouvoir activer CloudTrail Insights, vous pouvez

consulter les événements Insights enregistrés dans votre suivi tant que vous les stockez dans le compartiment S3 configuré dans les paramètres de suivi.

Surveillez vos journaux de suivi et soyez averti lorsque des événements spécifiques d'Insights se produisent avec Amazon CloudWatch Logs. Pour plus d'informations, consultez Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.

Pour afficher les événements Insights

CloudTrail Les événements Insights doivent être activés sur votre parcours pour voir les événements Insights dans la console. Prévoyez jusqu'à 36 heures CloudTrail pour diffuser les premiers événements Insights, si une activité inhabituelle est détectée.

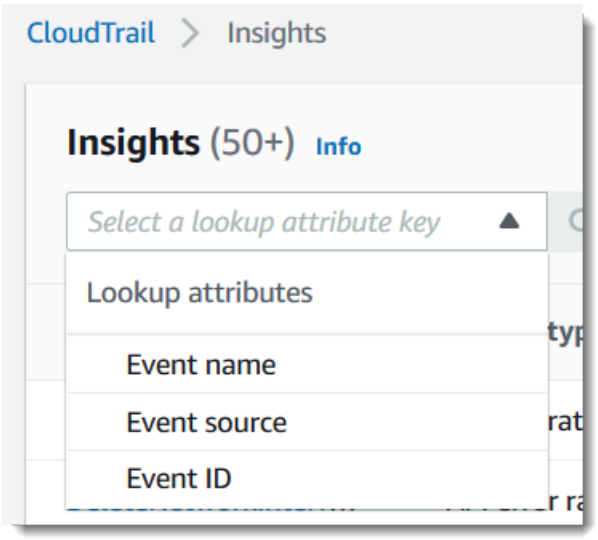
1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/home/.
2. Dans le volet de navigation, choisissez Dashboard (Tableau de bord) pour voir les cinq événements Insights les plus récents ou Insights pour voir tous les événements Insights journalisés dans votre compte au cours des 90 derniers jours.

   Sur la page Insights, vous pouvez filtrer les événements Insights par critères, dont la source de l'API d'événement, le nom et l'ID de l'événement, mais aussi limiter les événements affichés à ceux correspondant à une plage de temps spécifique. Pour plus d'informations sur le filtrage des événements Insights, consultez Filtrage des événements Insights.

Table des matières

Filtrage des événements Insights

L'affichage par défaut des événements dans Insights présente les événements dans l'ordre chronologique inverse. Les événements Insights les plus récents, triés par heure de début de l'événement, figurent en premier. La liste suivante décrit les attributs disponibles. Vous pouvez filtrer les trois premiers attributs :Nom de l'événement, Source de l'événement, et ID de l'événement.



Nom de l'événement

Le nom de l'événement, généralement l' AWS API sur laquelle des niveaux d'activité inhabituels ont été enregistrés.

Type Insight

Type d'événement CloudTrail Insights, qui est soit le taux d'appels d'API, soit le taux d'erreur d'API. Le type Insight relatif aux Taux d'appels d'API analyse les appels des API de gestion en écriture seule qui sont agrégés par minute par rapport à un volume d'appels des API de référence. Le type Insight relatif aux Taux d'erreur de l'API analyse les appels des API de gestion qui génèrent des codes d'erreur. L'erreur s'affiche en cas d'échec de l'appel d'API.

Source de l'événement

Le AWS service auquel la demande a été adressée, tel que `iam.amazonaws.com` ou `s3.amazonaws.com`. Vous pouvez faire défiler la liste des sources d'événements après avoir choisi le filtre Source de l'événement.

ID de l'événement

L'ID de l'événement Insights. Les ID de l'événement ne sont pas affichés dans le tableau de la page Insights, mais ils constituent un attribut sur lequel vous pouvez filtrer des événements Insights. Les ID de l'événement des événements de gestion qui sont analysés pour générer des événements Insights sont différents des ID de l'événement des événements Insights.

Heure de début de l'événement

L'heure de début de l'événement Insights, mesuré sous la forme de la première minute au cours de laquelle une activité d'API inhabituelle a été enregistrée. Cet attribut est affiché dans la table Insights, mais vous ne pouvez pas filtrer l'heure de début de l'événement dans la console.

Moyenne de référence

Modèle normal de taux d'appels d'API ou d'activité de taux d'erreur. La référence est calculée sur les sept jours précédant le démarrage d'un événement Insights. Bien que la valeur de la durée de référence, c'est-à-dire la période d' CloudTrailanalyse de l'activité normale sur les API, soit d'environ sept jours, CloudTrail arrondie la durée de référence à un jour entier, de sorte que la durée de référence exacte peut varier.

Moyenne Insight

Le nombre moyen d'appels vers une API, ou le nombre moyen d'une erreur spécifique renvoyée lors d'appels à une API, qui a déclenché l'événement Insights. La moyenne d' CloudTrail Insights pour l'événement de démarrage est le taux d'occurrences qui ont déclenché l'événement Insights. Généralement, il s'agit de la première minute d'activité inhabituelle. La moyenne Insights pour l'événement de fin est le taux des occurrences pendant la durée de l'activité inhabituelle, entre l'événement Insights de démarrage et l'événement Insights de fin.

Variation du taux

Différence entre la valeur de Moyenne de référence et Moyenne Insight, mesurée en pourcentage. Par exemple, si la moyenne de référence d'une erreur `AccessDenied` est de 1,0, et la moyenne Insight est de 3,0, la variation du taux est de 300 %. Une variation du taux pour une moyenne Insight qui dépasse une moyenne de référence affiche une flèche vers le haut à côté de la valeur. Si l'événement Insights a été journalisé parce que l'activité est inférieure à la moyenne de référence, Variation du taux affiche une flèche vers le bas à côté du pourcentage.

Si aucun événement n'est journalisé pour l'attribut ou l'heure que vous avez choisi, la liste des résultats est vide. Vous pouvez appliquer un seul filtre d'attributs, en plus de la plage de temps. Si vous choisissez un autre filtre d'attribut, la plage de temps que vous avez spécifiée est conservée.

Les étapes suivantes expliquent comment filtrer sur les attributs.

Pour filtrer par attribut

1. Pour filtrer les résultats selon un attribut, sélectionnez Rechercher un attribut dans le menu déroulant, puis tapez ou sélectionnez une valeur dans la zone Enter a lookup value (Saisir la valeur à rechercher).
2. Pour supprimer un filtre d'attributs, cliquez sur la croix à droite de la zone de filtre d'attributs.

Les étapes suivantes expliquent comment filtrer sur une date et une heure de début et de fin.

Pour filtrer selon une date et une heure de début et de fin

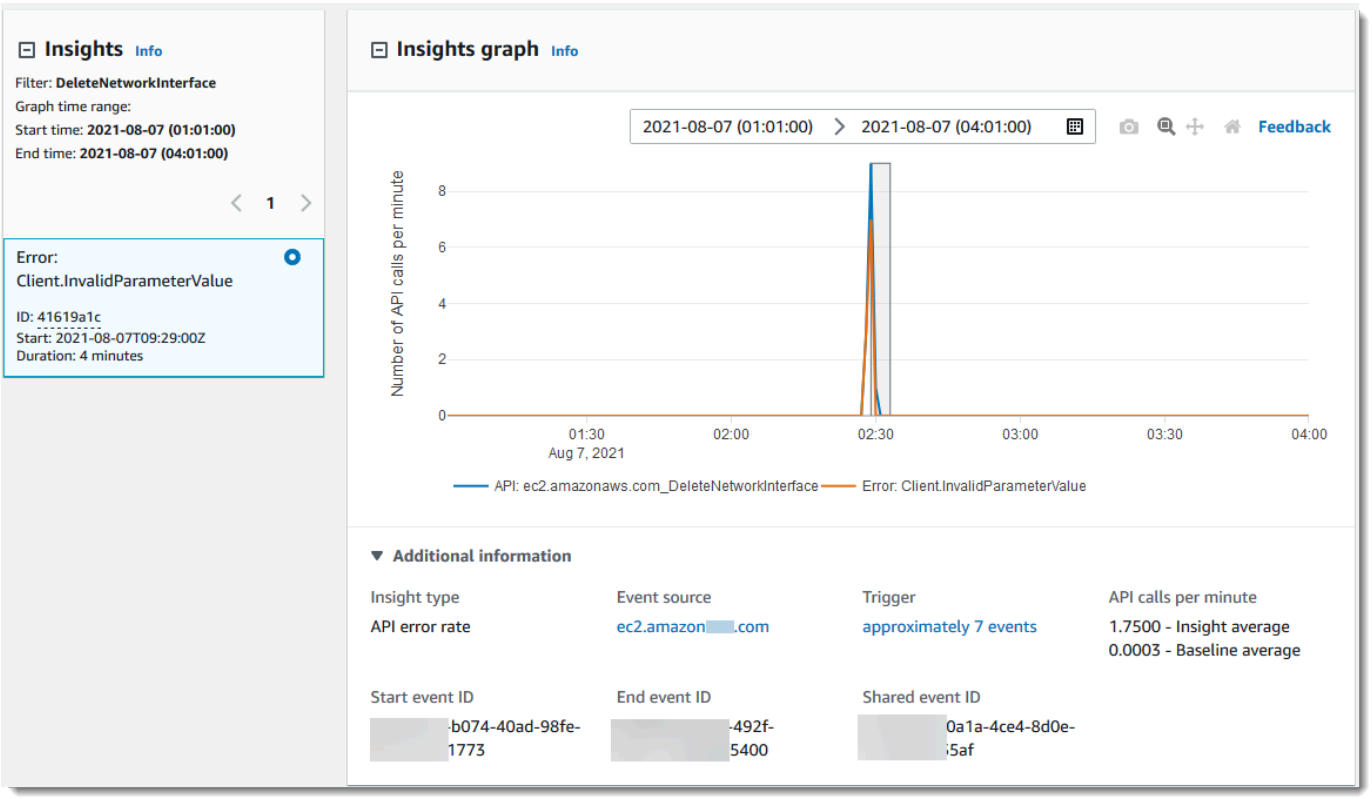
1. Pour restreindre la plage de temps pour les événements que vous voulez voir, choisissez une plage de temps dans la barre de temps en haut de la table. Les plages de temps prédéfinies incluent 30 minutes, 1 heure, 3 heures ou 12 heures. Pour spécifier une plage de temps personnalisée, choisissez Custom (Personnaliser).
2. Choisissez l'un des onglets suivants.
   - Absolute (Absolu)- Vous permet de choisir une heure spécifique. Passez à l'étape suivante.
   - Relatif à l'événement sélectionné- Sélectionné par défaut. Vous permet de choisir une période par rapport à l'heure de début d'un événement Insights. Passez à l'étape 4.
3. Pour définir une plage de temps Absolute (Absolu) , effectuez les opérations suivantes.
   a. Dans l'onglet Absolute (Absolu), choisissez le jour où vous souhaitez que la plage de temps démarre. Entrez une heure de début le jour sélectionné. Pour saisir une date manuellement, tapez la date dans le format `yyyy/mm/dd`. Les heures de début et de fin utilisent le format horaire de 24 heures, et les valeurs doivent être au format `hh:mm:ss`. Par exemple, pour indiquer que l'heure de début est 18 h 30, entrez **`18:30:00`**.
   b. Choisissez une date de fin pour la plage sur le calendrier, ou spécifiez une date et une heure de fin sous le calendrier. Choisissez Apply (Appliquer).
4. Pour définir une plage de temps Relative à l'événement sélectionné, procédez comme suit.
   a. Choisissez une période prédéfinie par rapport à l'heure de début des événements Insights. Les valeurs prédéfinies sont disponibles en minutes, heures, jours ou semaines. La période relative maximale est de 12 semaines.
   b. Si nécessaire, personnalisez la valeur prédéfinie dans les cases situées sous les paramètres prédéfinis. Choisissez Clear (Effacer) pour réinitialiser vos modifications si

nécessaire. Lorsque vous avez défini l'heure relative que vous souhaitez, choisissez Apply (Appliquer).

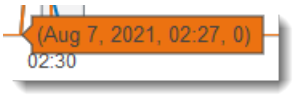
5. Dans To (À), choisissez le jour et spécifiez l'heure de la fin de la plage de temps. Choisissez Appliquer.
6. Pour supprimer un filtre de plage de temps, cliquez sur l'icône de calendrier à droite de la zone Time range (Plage de temps), puis choisissez Remove (Supprimer).

Affichage des détails des événements Insights

1. Choisissez un événement Insights dans la liste des résultats pour en afficher les détails. La page des détails d'un événement Insights présente un graphique de la chronologie d'activité inhabituelle.



2. Passez la souris sur les bandes en surbrillance pour afficher l'heure de début et la durée de chaque événement Insights dans le graphique.



Les informations suivantes sont présentées dans les Informations supplémentaires zone du graphique :

- Insight type (Type Insight). Il peut s'agir du taux d'appel d'API ou du taux d'erreur de l'API.
- Déclencheur. Ceci est un lien vers l'onglet CloudTrail events (Événements CloudTrail), qui répertorie les événements de gestion analysés par pour déterminer qu'une activité inhabituelle s'est produite.
- Appels d'API par minute
  - Baseline average (Moyenne de référence) : le taux typique d'occurrences par minute sur l'API sur laquelle l'événement Insights a été journalisé, tel que mesuré approximativement au cours des sept jours précédents, dans une région spécifique de votre compte.
  - Insights average (Moyenne Insights) : le taux des occurrences par minute à cette API ayant déclenché l'événement Insights. La moyenne d' CloudTrail Insights pour l'événement de démarrage est le taux d'appels ou d'erreurs par minute sur l'API qui a déclenché l'événement Insights. Généralement, il s'agit de la première minute d'activité inhabituelle. La moyenne Insights pour l'événement de fin est le taux d'appels d'API ou d'erreurs par minute pendant la durée de l'activité inhabituelle, entre l'événement Insights de démarrage et l'événement Insights de fin.
- Source de l'événement Point de terminaison du AWS service sur lequel le nombre inhabituel d'appels ou d'erreurs d'API a été enregistré. Dans l'image précédente, la source est `ec2.amazonaws.com`, qui constitue le point de terminaison de service pour Amazon EC2.
- ID de l'événement.
  - ID de l'événement de démarrage- ID de l'événement Insights journalisé au début d'une activité inhabituelle.
  - ID de l'événement de fin- ID de l'événement Insights journalisé à la fin d'une activité inhabituelle.
  - ID d'événement partagé : dans les événements Insights, l'ID d'événement partagé est un GUID généré par CloudTrail Insights pour identifier de manière unique une paire d'événements Insights de début et de fin. ID de l'événement partagé est commun entre l'événement Insights de début et de fin, et aide à créer une corrélation entre les deux événements pour identifier de manière unique l'activité inhabituelle.

3. Choisir l'onglet Attributions pour afficher des informations sur les identités utilisateur, les agents utilisateur et les évènements Insights de taux d'appel API, des codes d'erreur en corrélation avec une activité inhabituelle et de base. Un maximum de cinq identités d'utilisateur, de cinq agents

utilisateur et de cinq codes d'erreur sont affichés dans les tableaux de l'onglet Attributions, trié par une moyenne du nombre d'activités, dans l'ordre décroissant du plus haut au plus bas. Pour plus d'informations sur l'onglet Attributions, consultez Onglet Attributions et CloudTrail `insightDetails`Élément Insights dans ce guide.

4. Dans l'onglet CloudTrail Événements, consultez les événements connexes CloudTrail analysés pour déterminer qu'une activité inhabituelle s'est produite. Par défaut, un filtre est déjà appliqué pour le nom de l'événement Insights, qui est également le nom de l'API associée. L'onglet CloudTrail événements affiche les événements de CloudTrail gestion liés à l'API en question survenus entre l'heure de début (moins une minute) et l'heure de fin (plus une minute) de l'événement Insights.

   Lorsque vous sélectionnez d'autres événements Insights dans le graphique, les événements présentés dans le tableau CloudTrail des événements changent. Ces événements vous aident à effectuer une analyse plus approfondie afin de déterminer la cause probable d'un événement Insights et les raisons de l'activité inhabituelle de l'API.

   Pour afficher tous les CloudTrail événements enregistrés pendant la durée de l'événement Insights, et pas uniquement ceux relatifs à l'API associée, désactivez le filtre.

5. Cliquez sur l'onglet Insights event record (Enregistrement d'événement Insights) pour afficher les événements Insights de début et de fin au format JSON.

6. Le choix de la Event source (Source d'événement) liée vous renvoie à la page Insights, filtrée en fonction de cette source d'événement.

Zoomer, panoramiquer et télécharger un graphique

Vous pouvez zoomer, panoramiquer et réinitialiser les axes du graphique sur la page de détails de l'événement Insights à l'aide d'une barre d'outils située dans le coin supérieur droit.

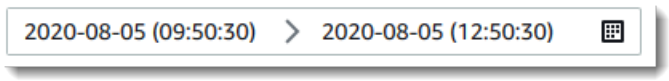
De gauche à droite, les boutons de commande de la barre d'outils de graphique permettent d'effectuer les opérations suivantes :

- Download plot as a PNG (Télécharger un diagramme au format PNG) - Téléchargez l'image graphique affichée sur la page des détails et enregistrez-la au format PNG.

- Zoom - Faites glisser la souris pour sélectionner une zone du graphique que vous souhaitez agrandir et voir plus en détail.
- Pan (Panoramiquer) - Déplacez le graphique pour voir les dates ou les heures adjacentes.
- Reset axes (Réinitialiser les axes) - Replacez les axes du graphique dans leur position d'origine, en supprimant les paramètres de zoom et de panoramique.

Modifier les paramètres de période du graphique

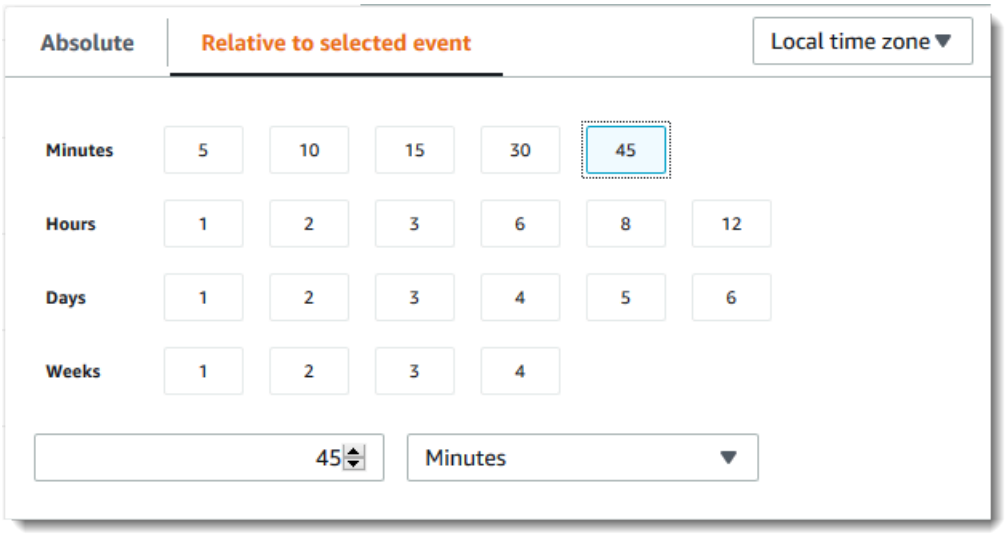
Vous pouvez modifier la période de temps, la durée sélectionnée des événements affichés dans l'axe x, qui s'affiche dans le graphique, en choisissant un paramètre dans le coin supérieur droit du graphique.



La période par défaut affichée dans le graphique dépend de la durée de l'événement Insights sélectionné.

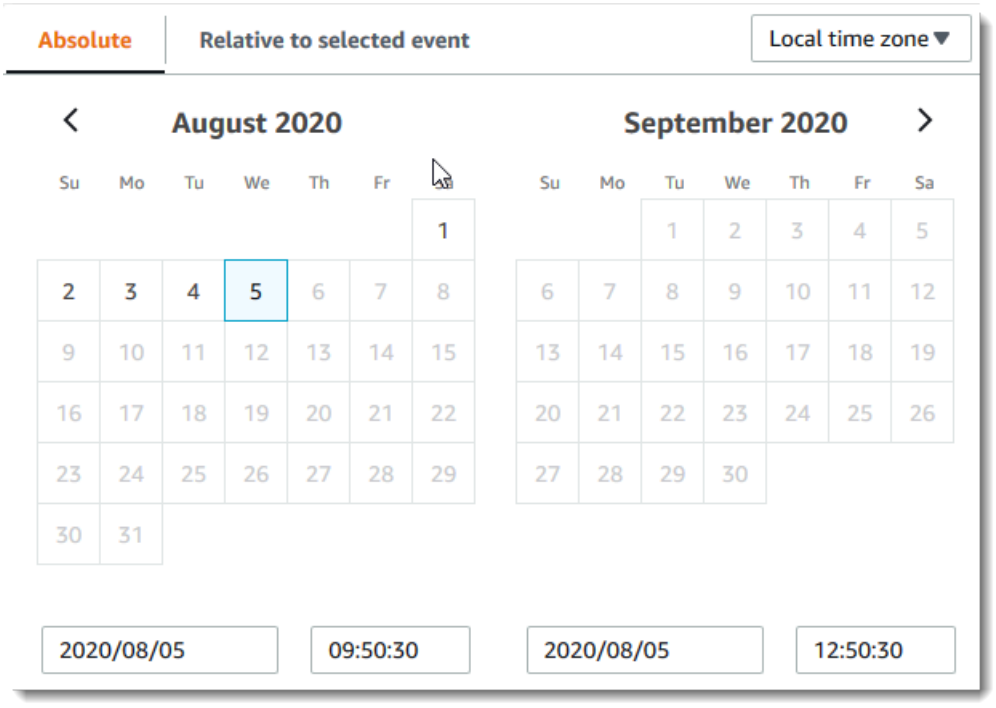
Durée de l'événement Insights	Période par défaut
Moins de 4 heures	3h (trois heures)
Entre 4 et 12 heures	12h(12 heures)
Entre 12 et 24 heures	1d (un jour)
Entre 24 et 72 heures	3d (trois jours)
Plus de 72 heures	1w (une semaine)

Vous pouvez choisir des préréglages de cinq minutes, 30 minutes, une heure, trois heures, 12 heures ou Custom (Personnaliser). L'image suivante montre les périodes relatives à l'événement sélectionné que vous pouvez choisir dans les paramètres Custom (Personnaliser). Les périodes relatives sont des périodes approximatives entourant le début et la fin de l'événement Insights sélectionné qui s'affiche sur la page de détails d'un événement Insights.



Pour personnaliser un préréglage sélectionné, spécifiez un nombre et une unité de temps dans les zones situées sous les préréglages.

Pour spécifier une plage de dates et d'heures exactes, choisissez l'onglet Absolute (Absolu). Si vous définissez une plage de dates et d'heures absolues, les heures de début et de fin seront requises. Pour plus d'informations sur comment définir l'heure, consultez the section called "Filtrage des événements Insights" dans cette rubrique.



Téléchargement d'événements Insights

Vous pouvez télécharger l'historique des événements Insights enregistrés en tant que fichier au format JSON ou CSV. Utilisez des filtres et des plages de temps pour réduire la taille du fichier que vous téléchargez.

> **Note**
>
> CloudTrail les fichiers d'historique des événements sont des fichiers de données qui contiennent des informations (telles que les noms des ressources) qui peuvent être configurées par des utilisateurs individuels. Certaines données peuvent éventuellement être interprétées comme des commandes dans des programmes utilisés pour lire et analyser ces données (injection CSV). Par exemple, lorsque CloudTrail des événements sont exportés au format CSV et importés dans un tableur, ce programme peut vous avertir de problèmes de sécurité. Comme bonne pratique relative à la sécurité, désactivez les liens ou les macros des fichiers d'historique des événements téléchargés.

1. Spécifiez le filtre et la plage de temps pour les événements que vous souhaitez télécharger. Par exemple, vous pouvez spécifier le nom d'événement, `StartInstances`, et indiquer une plage de temps pour les trois derniers jours d'activité.
2. Choisissez Download events (Télécharger les événements), puis choisissez Download CSV (Télécharger au format CSV) ou Download JSON ((Télécharger au format JSON). Vous êtes invité à choisir un emplacement pour enregistrer le fichier.

   > **Note**
   >
   > Le téléchargement pourrait prendre un certain temps. Pour des résultats plus rapides, utilisez un filtre spécifique ou une plage de temps plus courte pour affiner les résultats avant de commencer le processus de téléchargement.

3. Une fois le téléchargement terminé, ouvrez le fichier pour afficher les événements que vous avez spécifiés.
4. Pour annuler votre téléchargement, choisissez Cancel download (Annuler le téléchargement). Si vous annulez un téléchargement avant qu'il ne soit terminé, un fichier CSV ou JSON se trouvant sur votre ordinateur local pourrait contenir seulement une partie de vos événements.

Visualisation CloudTrail des événements Insights pour les sentiers avec AWS CLI

Vous pouvez consulter les événements CloudTrail Insights des 90 derniers jours en exécutant la aws cloudtrail lookup-events commande. La commande `lookup-events` dispose des options suivantes :

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

Pour obtenir des informations générales sur l'utilisation du AWS Command Line Interface, consultez le guide de AWS Command Line Interface l'utilisateur.

Table des matières

Prérequis

- Pour exécuter AWS CLI des commandes, vous devez installer le AWS CLI. Pour plus d'informations, voir Commencer avec le AWS CLI.
- Assurez-vous que votre AWS CLI version est supérieure à 1.6.6. Pour vérifier la version de la CLI, exécutez aws --version sur la ligne de commande.
- Pour définir le compte, la région et le format de sortie par défaut pour une AWS CLI session, utilisez la aws configure commande. Pour plus d'informations, consultez Configuration de l'interface de ligne de commande AWS.
- Pour enregistrer les événements Insights sur le volume d'appels des API, le journal doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, le journal de suivi doit enregistrer les événements de gestion `read` ou `write`.

> **Note**
>
> Les CloudTrail AWS CLI commandes distinguent les majuscules et minuscules.

Obtenir de l'aide de la ligne de commande

Pour voir l'aide de la ligne de commande pour `lookup-events`, tapez la commande suivante.

```
aws cloudtrail lookup-events help
```

Recherche d'événements Insights

Pour voir les dix derniers événements Insights, tapez la commande suivante :

```
aws cloudtrail lookup-events --event-category insight
```

Un événement renvoyé ressemble à l'exemple suivant,

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.07",
```

```
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
```

```
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      },
      {
          "eventVersion": "1.07",
          "eventTime": "2019-10-15T21:14:00Z",
```

```
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "End",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
```

```
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "userAgent",
                    "insight": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "errorCode",
                    "insight": [
                      {
                        "value": "null",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "null",
                        "average": 0.0000882145
                      }
                    ]
                  }
                ]
              }
            },
              "eventCategory": "Insight"
          }
      ]
}
```

Pour une explication des champs liés à la recherche dans la sortie, consultez Champs de résultat de la recherche dans cette rubrique. Pour une explication sur les champs de l'événement Insights, consultez CloudTrail enregistrer le contenu.

Spécification du nombre d'événements Insights à renvoyer

Pour spécifier le nombre d'événements à renvoyer, saisissez la commande suivante.

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

La valeur par défaut pour *<integer>*, si elle n'est pas spécifiée, est 10. Les valeurs possibles vont de 1 à 50. L'exemple suivant renvoie un résultat.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

Recherche d'événements Insights par plage de temps

Les événements Insights survenus au cours des 90 derniers jours sont disponibles pour la recherche. Pour spécifier une plage de temps, saisissez la commande suivante.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>* spécifie, en UTC, que seuls les événements Insights qui se produisent au moment indiqué ou après sont renvoyés. Si l'heure de début spécifiée survient après l'heure de fin spécifiée, une erreur est renvoyée.

`--end-time` *<timestamp>* spécifie, en UTC, que seuls les événements Insights qui se produisent au moment indiqué ou avant sont renvoyés. Si l'heure de fin spécifiée survient avant l'heure de début spécifiée, une erreur est renvoyée.

L'heure de début par défaut est la première date à laquelle les données sont disponibles au cours des 90 derniers jours. L'heure de fin par défaut est l'heure de l'événement qui s'est produit le plus près de l'heure actuelle.

Tous les horodatages sont affichés en UTC.

Recherche d'événements Insights par attribut

Pour filtrer selon un attribut, tapez la commande suivante.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Vous ne pouvez spécifier qu'une seule paire clé-valeur d'attribut pour chaque commande lookup-events. Les valeurs d'événement Insights valides pour `AttributeKey` sont les suivants. Les noms de valeur sont sensibles à la casse.

- `EventId`
- `EventName`
- `EventSource`

La longueur maximale du `AttributeValue` est de 2 000 caractères. Les caractères suivants (« _ », « », « , », « \\n ») comptent pour deux caractères dans la limite de 2000 caractères.

Exemples de recherche d'attribut

L'exemple de commande suivant renvoie les événements Insights dans lesquels la valeur de `EventName` est `PutRule`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

L'exemple de commande suivant renvoie les événements Insights dans lesquels la valeur de `EventId` est `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

L'exemple de commande suivant renvoie les événements Insights dans lesquels la valeur de `EventSource` est `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

Spécifier la page de résultats suivante

Pour obtenir la page de résultats suivante à partir d'une commande `lookup-events`, saisissez la commande suivante.

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

Dans cette commande, la valeur de *<token>* provient du premier champ de la sortie de la commande précédente.

Lorsque vous utilisez `--next-token` dans une commande, vous devez utiliser les mêmes paramètres que dans la commande précédente. Par exemple, supposons que vous exécutiez la commande suivante.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Pour obtenir la page de résultats suivante, votre commande suivante se présente comme suit.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

Extraction de l'entrée JSON d'un fichier

AWS CLI Pour certains AWS services, il existe deux paramètres, l'un `--generate-cli-skeleton` et l'autre`--cli-input-json`, que vous pouvez utiliser pour générer un modèle JSON, que vous pouvez modifier et utiliser comme entrée pour le `--cli-input-json` paramètre. Cette section décrit comment utiliser ces paramètres avec `aws cloudtrail lookup-events`. Pour plus d'informations, consultez les AWS CLI squelettes et les fichiers d'entrée.

Pour rechercher des événements Insights en extrayant une entrée JSON d'un fichier

1. Créer un modèle d'entrée à utiliser avec `lookup-events` en redirigeant la sortie de `--generate-cli-skeleton` vers un fichier, comme dans l'exemple suivant.

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   Le fichier modèle généré (dans ce cas, LookupEvents .txt) ressemble à ce qui suit.

   ```
   {
   ```

```
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Utilisez un éditeur de texte pour modifier le code JSON le cas échéant. L'entrée JSON doit contenir uniquement des valeurs qui sont spécifiées.

> **Important**
>
> Toutes les valeurs vides ou null doivent être supprimées du modèle pour que vous puissiez l'utiliser.

L'exemple suivant spécifie un intervalle de temps et un nombre maximal de résultats à retourner.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Pour utiliser le fichier modifié en tant qu'entrée, utilisez la syntaxe `--cli-input-json file://<nom de fichier>`, comme dans l'exemple suivant.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> Vous pouvez utiliser d'autres arguments sur la même ligne de commande en tant que `--cli-input-json`.

Champs de résultat de la recherche

Evénements

Liste des événements de recherche basée sur l'attribut de recherche et la plage de temps qui ont été spécifiés. La liste des événements est triée par heure, le dernier événement arrivant en tête. Chaque entrée contient des informations sur la demande de recherche et inclut une représentation sous forme de chaîne de l' CloudTrail événement récupéré.

Les entrées suivantes décrivent les champs dans chaque événement de recherche.

CloudTrailEvent

Chaîne JSON qui contient une représentation d'objet de l'événement renvoyé. Pour plus d'informations sur chacun des éléments renvoyés, consultez Contenu du corps d'un enregistrement.

EventId

Chaîne qui contient le GUID de l'événement retourné.

EventName

Chaîne qui contient le nom de l'événement renvoyé.

EventSource

Le AWS service auquel la demande a été adressée.

EventTime

Date et heure, au format de temps UNIX, de l'événement.

Ressources

Liste de ressources référencées par l'événement qui a été renvoyé. Chaque entrée de ressource spécifie un type de ressource et un nom de ressource.

ResourceName

Chaîne qui contient le nom de la ressource référencée par l'événement.

ResourceType

Chaîne qui contient le type d'une ressource référencée par l'événement. Lorsque le type de ressource ne peut pas être déterminé, la valeur null est renvoyée.

Username

Chaîne qui contient le nom d'utilisateur du compte pour l'événement renvoyé.

NextToken

Chaîne pour obtenir la page de résultats suivante d'une commande `lookup-events` précédente. Pour utiliser le jeton, les paramètres doivent être identiques à ceux de la commande d'origine. Si aucune entrée `NextToken` n'apparaît dans la sortie, cela signifie qu'il n'y a aucun résultat à renvoyer.

Pour plus d'informations sur CloudTrail les événements Insights, consultez Journalisation des événements Insights ce guide.

Copier les événements du sentier sur CloudTrail le lac

Vous pouvez copier les événements de randonnée existants dans un magasin de données d'événements CloudTrail Lake pour créer un point-in-time instantané des événements enregistrés sur le sentier. La copie des événements du journal de suivi n'interfère pas avec la capacité du journal de suivi à journaliser les événements et ne modifie en aucune façon le journal.

Vous pouvez copier les événements de suivi dans un magasin de données d'événements existant configuré pour les CloudTrail événements, ou vous pouvez créer un nouveau magasin de données d' CloudTrail événements et choisir l'option Copier les événements de suivi dans le cadre de la création du magasin de données d'événements. Pour plus d'informations sur la copie des événements de suivi dans un entrepôt de données d'événement existant, veuillez consulter Copiez les événements de suivi dans un magasin de données d'événements existant à l'aide de la CloudTrail console. Pour plus d'informations sur la création d'un entrepôt de données d'événement, veuillez consulter Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

La copie des événements de suivi dans un magasin de données d'événements CloudTrail Lake vous permet d'exécuter des requêtes sur les événements copiés. CloudTrail Les requêtes Lake offrent une vue plus approfondie et plus personnalisable des événements que de simples recherches de clés et de valeurs dans l'historique des événements ou en cours d'exécution`LookupEvents`. Pour plus d'informations sur CloudTrail Lake, voirTravailler avec AWS CloudTrail Lake.

Si vous copiez des événements de journal de suivi vers le magasin de données d'événement d'une organisation, vous devez utiliser le compte de gestion de l'organisation. Vous ne pouvez pas copier les événements de journal de suivi en utilisant le compte administrateur délégué d'une organisation.

CloudTrail Les magasins de données sur les événements de Lake sont payants. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification et la gestion des coûts du lac, voir AWS CloudTrail Tarification etGestion des coûts CloudTrail du lac.

Lorsque vous copiez des événements de parcours dans un magasin de données d'événements CloudTrail Lake, vous êtes facturé en fonction de la quantité de données non compressées ingérée par le magasin de données d'événements.

Lorsque vous copiez des événements de suivi dans CloudTrail Lake, CloudTrail décompressez les journaux stockés au format gzip (compressé), puis copie les événements contenus dans les journaux dans votre magasin de données d'événements. La taille des données non compressées peut être supérieure à la taille réelle du stockage S3. Pour obtenir une estimation générale de la taille des données non compressées, vous pouvez multiplier par 10 la taille des journaux du compartiment S3.

Vous pouvez réduire les coûts en spécifiant une plage de temps plus restreinte pour les événements copiés. Si vous prévoyez de n'utiliser l'entrepôt de données d'événement que pour interroger vos événements copiés, vous pouvez désactiver l'ingestion des événements afin d'éviter d'encourir des frais lors d'événements futurs. Pour plus d'informations, veuillez consulter Tarification AWS CloudTrail et Gestion des coûts CloudTrail du lac.

Scénarios

Le tableau suivant décrit certains scénarios courants de copie d'événements de suivi et explique comment réaliser chaque scénario à l'aide de la console.

Scénario	Comment puis-je y parvenir dans la console ?
Analysez et interrogez les événements historiques des sentiers dans CloudTrail le lac sans ingérer de nouveaux événements	Créez un nouveau magasin de données d'événement et choisissez l'option Copier les événements de suivi dans le cadre de la création du magasin de données d'événement. Lorsque vous créez le magasin de données d'événement, désélectionnez Ingérer les événements (étape 15 de la procédure) pour vous assurer que le magasin de données d'événement ne contient que les événements passés de votre journal de suivi et aucun événement futur.

Scénario	Comment puis-je y parvenir dans la console ?
Remplacez votre parcours existant par un magasin de données sur les événements CloudTrail Lake	Créez un entrepôt de données d'événement avec les mêmes sélecteurs d'événements que votre journal de suivi pour vous assurer que l'entrepôt de données d'événement a la même couverture que votre journal de suivi. Pour éviter de dupliquer les événements entre le journal de suivi source et l'entrepôt de données d'événement de destination, choisissez pour les événements copiés une plage de temps antérieure à la création de l'entrepôt de données d'événement. Une fois l'entrepôt de données d'événement créé, vous pouvez désactiver la journalisation du journal de suivi pour éviter des frais supplémentaires.

Rubriques

Considérations pour copier les événements de journal de suivi

Tenez compte des facteurs suivants lors de la copie d'événements du journal de suivi.

- Lorsque vous copiez des événements de CloudTrail suivi, utilise l'opération d'`GetObject`API S3 pour récupérer les événements de suivi dans le compartiment S3 source. Certaines classes de stockage S3, telles que les niveaux S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts et S3 Intelligent-Tiering Deep Archive ne sont pas accessibles en utilisant `GetObject`. Pour copier les événements de suivi stockés dans ces classes de stockage archivées, vous devez d'abord restaurer une copie à l'aide de l'opération S3 `RestoreObject`. Pour plus d'informations sur la restauration d'objets archivés, veuillez consulter Restauration d'un objet archivé dans le Guide de l'utilisateur Amazon S3.
- Lorsque vous copiez des événements de suivi dans un magasin de données d'événements, CloudTrail copie tous les événements de suivi, quelle que soit la configuration des types

d'événements, des sélecteurs d'événements avancés ou Région AWS de la banque de données de destination.

- Avant de copier les événements de suivi dans un magasin de données d'événement existant, assurez-vous que l'option de tarification et la période de conservation du magasin de données d'événement sont configurées de manière appropriée pour votre cas d'utilisation.
  - Option de tarification : l'option de tarification détermine le coût d'ingestion et de stockage des événements. Pour de plus amples informations sur les options de tarification, consultez Tarification d'AWS CloudTrail et Options de tarification du magasin de données d'événement.
  - Période de conservation : La période de conservation détermine la durée pendant laquelle les données d'événements sont conservées dans le magasin de données d'événements. CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.
- Si vous copiez des événements de journal de suivi vers un magasin de données d'événement à des fins d'investigation et que vous ne souhaitez pas ingérer d'événements futurs, vous pouvez arrêter l'ingestion dans le magasin de données d'événement. Lorsque vous créez le magasin de données d'événement, désélectionnez l'option Ingérer les événements (étape 15 de la procédure) pour vous assurer que le magasin de données d'événement ne contient que les événements passés de votre journal de suivi et aucun événement futur.
- Avant de copier les événements du journal de suivi, désactivez toutes les listes de contrôle d'accès (ACL) associées au compartiment S3 source et mettez à jour la politique du compartiment S3 pour le magasin de données d'événement de destination. Pour plus d'informations sur la mise à jour de la politique de compartiment S3, veuillez consulter Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi. Pour plus d'informations sur la désactivation des listes ACL, veuillez consulter la rubrique Contrôle de la propriété des objets et désactivation des listes ACL pour votre compartiment.
- CloudTrail copie uniquement les événements de suivi à partir des fichiers journaux compressés Gzip qui se trouvent dans le compartiment S3 source. CloudTrail ne copie pas les événements

de suivi à partir de fichiers journaux non compressés ou de fichiers journaux compressés dans un format autre que Gzip.

- Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez pour les événements copiés une plage de temps antérieure à la création du magasin de données d'événement.
- Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, vous devez choisir le préfixe lorsque vous copiez des événements de suivi.
- Pour copier les événements de journal de suivi vers le magasin de données d'événement d'une organisation, vous devez utiliser le compte de gestion de l'organisation. Vous ne pouvez pas utiliser le compte d'administrateur délégué pour copier des événements de journal de suivi vers le magasin de données d'événement d'une organisation.

Autorisations requises pour copier les événements de journal de suivi

Avant de copier des événements de suivi, assurez-vous de disposer de toutes les autorisations requises pour votre rôle IAM. Vous devez uniquement mettre à jour les autorisations du rôle IAM si vous choisissez un rôle IAM existant pour copier les événements de journal de suivi. Si vous choisissez de créer un nouveau rôle IAM, CloudTrail fournit toutes les autorisations nécessaires pour ce rôle.

Si le compartiment S3 source utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique de clé KMS autorise CloudTrail le déchiffrement des données du compartiment. Si le compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé CloudTrail pour autoriser le déchiffrement des données du compartiment.

Rubriques

- Autorisations IAM pour copier les événements de journal de suivi
- Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi
- Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source

Autorisations IAM pour copier les événements de journal de suivi

Lorsque vous copiez des événements de journal de suivi, vous pouvez créer un nouveau rôle IAM ou utiliser un rôle IAM existant. Lorsque vous choisissez un nouveau rôle IAM, vous CloudTrail créez un rôle IAM avec les autorisations requises et aucune autre action n'est requise de votre part.

Si vous choisissez un rôle existant, assurez-vous que les politiques du rôle IAM autorisent la copie CloudTrail des événements de suivi depuis le compartiment S3 source. Cette section fournit des exemples de politiques d'approbation et d'autorisation requises du rôle IAM.

L'exemple suivant fournit la politique d'autorisation, qui permet CloudTrail de copier les événements de suivi depuis le compartiment S3 source. Remplacez *myBucketNameMyAccountId*, *region*, *prefix* et *eventDataStoreId* par les valeurs appropriées à votre configuration. Le *MyAccountID* est l'ID de AWS compte utilisé pour CloudTrail Lake, qui peut être différent de l'ID de AWS compte du compartiment S3.

Remplacez *key-region*, *keyAccountID* et *keyID* par les valeurs de la clé KMS utilisée pour chiffrer le compartiment S3 source. Vous pouvez omettre l'instruction `AWSCloudTrailImportKeyAccess` si le compartiment S3 source n'utilise pas de clé KMS pour le chiffrement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
```

```
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

L'exemple suivant fournit la politique de confiance IAM, qui permet d' CloudTrail assumer un rôle IAM pour copier les événements de suivi depuis le compartiment S3 source. Remplacez *MyAccountId*, *region* et *eventDataStoreId* par les valeurs appropriées à votre configuration. Le *MyAccountID* est l'ID de AWS compte utilisé pour CloudTrail Lake, qui peut être différent de l'ID de AWS compte du compartiment S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
```

```
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi

Par défaut, les objets et les compartiments Amazon S3 sont privés. Seul le propriétaire de la ressource (le compte AWS qui a créé le compartiment) peut accéder au compartiment et aux objets qu'il contient. Le propriétaire de la ressource peut accorder des autorisations d'accès à d'autres ressources et à d'autres utilisateurs en créant une stratégie d'accès.

Avant de copier les événements de suivi, vous devez mettre à jour la politique du compartiment S3 CloudTrail pour autoriser la copie des événements de suivi depuis le compartiment.

Vous pouvez ajouter l'instruction suivante à la politique du compartiment S3 pour accorder ces autorisations. Remplacez *roLearn* et *myBucketName*par les valeurs appropriées à votre configuration.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source

Si le compartiment S3 source utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique de clé KMS fournit CloudTrail les `kms:GenerateDataKey` autorisations `kms:Decrypt` et les autorisations nécessaires pour copier les événements de suivi depuis un compartiment S3 avec le chiffrement SSE-KMS activé. Si votre compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la stratégie de chaque clé. La mise à jour de la politique des clés KMS permet CloudTrail de déchiffrer les données dans le compartiment S3 source, d'exécuter des contrôles de validation pour s'assurer que les événements sont conformes aux CloudTrail normes et de copier les événements dans le magasin de données d'événements CloudTrail Lake.

L'exemple suivant fournit la politique de clé KMS, qui permet CloudTrail de déchiffrer les données dans le compartiment S3 source. Remplacez *roLearn myBucketName*, *MyAccountId*, *region* et *eventDataStoreId* par les valeurs appropriées à votre configuration. Le *MyAccountID* est l'ID de AWS compte utilisé pour CloudTrail Lake, qui peut être différent de l'ID de AWS compte du compartiment S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Copiez les événements de suivi dans un magasin de données d'événements existant à l'aide de la CloudTrail console

Utilisez la procédure suivante pour copier les événements du journal de suivi vers un magasin de données d'événement existant. Pour plus d'informations sur la création d'un nouveau magasin de données d'événement, veuillez consulter Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

> **Note**
>
> Avant de copier les événements de suivi dans un magasin de données d'événement existant, assurez-vous que l'option de tarification et la période de conservation du magasin de données d'événement sont configurées de manière appropriée pour votre cas d'utilisation.
>
> - Option de tarification : l'option de tarification détermine le coût d'ingestion et de stockage des événements. Pour de plus amples informations sur les options de tarification, consultez Tarification d'AWS CloudTrail et Options de tarification du magasin de données d'événement.
> - Période de conservation : La période de conservation détermine la durée pendant laquelle les données d'événements sont conservées dans le magasin de données d'événements. CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Pour déterminer la période de conservation appropriée, additionnez l'événement le plus ancien que vous souhaitez copier en jours et le nombre de jours pendant lesquels vous souhaitez conserver les événements dans le magasin de données d'événements (période de conservation = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Par exemple, si l'événement le plus ancien que vous copiez date de 45 jours et que vous souhaitez conserver les événements dans le magasin de données d'événement pendant 45 jours supplémentaires, vous devez définir la période de conservation sur 90 jours.

Pour copier des événements de journal de suivi dans un magasin de données d'événement

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Choisissez Trails dans le volet de navigation gauche de la CloudTrail console.

3. Sur la page Journaux de suivi, sélectionnez le journal de suivi, puis Copier les événements vers Lake. Si le compartiment S3 source pour le suivi utilise une clé KMS pour le chiffrement des données, assurez-vous que la politique en matière de clés KMS autorise CloudTrail le déchiffrement des données du compartiment. Si le compartiment S3 source utilise plusieurs clés KMS, vous devez mettre à jour la politique de chaque clé CloudTrail pour autoriser le déchiffrement des données du compartiment. Pour plus d'informations sur la mise à jour de la stratégie de clé KMS, veuillez consulter Stratégie de clé KMS pour le déchiffrement des données dans le compartiment S3 source.
4. (Facultatif) Par défaut, copie CloudTrail uniquement les CloudTrail événements contenus dans le préfixe du compartiment S3 et `CloudTrail` les préfixes contenus dans le `CloudTrail` préfixe, et ne vérifie pas les préfixes des autres services. AWS Si vous souhaitez copier CloudTrail des événements contenus dans un autre préfixe, choisissez Enter S3 URI, puis Browse S3 pour accéder au préfixe.

   La politique du compartiment S3 doit autoriser CloudTrail l'accès pour copier les événements de suivi. Pour plus d'informations sur la mise à jour de la politique de compartiment S3, veuillez consulter Politique de compartiment Amazon S3 pour la copie d'événements de journal de suivi.
5. Pour Spécifier une plage temporelle d'événements, choisissez la plage de temps pour copier les événements. CloudTrail vérifie le préfixe et le nom du fichier journal pour vérifier que le nom contient une date comprise entre les dates de début et de fin choisies avant de tenter de copier les événements de suivi. Vous avez le choix entre Plage relative ou Plage absolue. Pour éviter de dupliquer les événements entre le journal de suivi source et le magasin de données d'événement de destination, choisissez une plage de temps antérieure à la création du magasin de données d'événement.

   > **Note**
   >
   > CloudTrail copie uniquement les événements de suivi dont la durée de conservation est `eventTime` conforme à la période de conservation de la banque de données d'événements. Par exemple, si la période de conservation d'un magasin de données d'événements est de 90 jours, aucun événement de suivi datant de `eventTime` plus de 90 jours ne CloudTrail sera copié.

   - Si vous choisissez Plage relative, vous pouvez choisir de copier les événements enregistrés au cours des 6 derniers mois, 1 an, 2 ans, 7 ans ou une plage personnalisée. CloudTrail copie les événements enregistrés pendant la période choisie.

- Si vous choisissez la plage absolue, vous pouvez choisir une date de début et de fin spécifique. CloudTrail copie les événements survenus entre les dates de début et de fin choisies.

6. Pour Lieu de diffusion, sélectionnez le magasin de données d'événement de destination dans la liste déroulante.
7. Pour Autorisations, sélectionnez l'une des options de rôle IAM suivantes. Si vous choisissez un rôle IAM existant, vérifiez que la politique de rôle IAM fournit les autorisations nécessaires. Pour plus d'informations sur la mise à jour des autorisations du rôle IAM, consultez Autorisations IAM pour copier les événements de journal de suivi.

   - Sélectionnez Créer un nouveau rôle (recommandé) pour créer un nouveau rôle IAM. Pour Enter IAM role name (Saisir le nom du rôle IAM), saisissez un nom pour le rôle. CloudTrail crée automatiquement les autorisations nécessaires pour ce nouveau rôle.
   - Choisissez Utiliser un ARN de rôle IAM personnalisé pour utiliser un rôle IAM personnalisé qui n'est pas répertorié. Pour Enter IAM role ARN (Saisir l'ARN du rôle IAM), saisissez l'ARN IAM.
   - Choisissez un rôle IAM existant dans la liste déroulante.
8. Choisissez Copy events (Copier les événements).
9. Une confirmation de copie vous est demandée. Dès que vous souhaitez confirmer, sélectionnez Copy trail events to Lake (Copier les événements du journal de suivi sur Lake), puis Copy events (Copier les événements).
10. Sur la page Copy details (Copier les détails), vous pouvez consulter le statut de la copie et les échecs éventuels. Lorsque la copie d'un événement de journal de suivi est terminée, son Copy status (Statut de la copie) est défini sur Completed (Terminé) si aucune erreur n'est survenue, ou Failed (Échec) si des erreurs sont survenues.

    > **Note**
    >
    > Les détails affichés sur la page des détails de la copie d'événement ne sont pas en temps réel. Les valeurs réelles des détails tels que les Prefixes copied (Préfixes copiés) peuvent être plus élevées que ce qui est indiqué sur la page. CloudTrail met à jour les détails progressivement au cours de la copie de l'événement.

11. Si le Statut de la copie est Échec, corrigez les erreurs qui s'affichent dans Échecs de la copie, puis sélectionnez Réessayer la copie. Lorsque vous réessayez d'effectuer une copie, elle CloudTrail reprend à l'endroit où l'échec s'est produit.

Pour plus d'informations sur l'affichage des informations relatives à la copie d'un événement de journal de suivi, veuillez consulter Informations de copie d'événement.

Obtenir et consulter vos fichiers CloudTrail journaux

Une fois que vous avez créé et configuré un journal d'activité pour capturer les fichiers journaux que vous souhaitez recevoir, vous devez pouvoir trouver les fichiers journaux et interpréter les informations qu'ils contiennent.

CloudTrail envoie vos fichiers journaux dans un compartiment Amazon S3 que vous spécifiez lors de la création du journal. CloudTrail fournit généralement des journaux dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti. Pour plus d'informations, consultez le Contrat de niveau de service (SLA)AWS CloudTrail. Les événements Insights sont généralement livrés dans votre compartiment dans les 30 minutes qui suivent une activité inhabituelle. Lorsque vous activez les événements Insights pour la première fois, prévoyez jusqu'à 36 heures pour voir les premiers événements Insights, si une activité inhabituelle est détectée.

> **Note**
>
> Si vous configurez mal votre trace (par exemple, si le compartiment S3 est inaccessible), vous CloudTrail tenterez de remettre les fichiers journaux à votre compartiment S3 pendant 30 jours, et ces attempted-to-deliver événements seront soumis aux frais standard. CloudTrail Pour éviter des frais sur un journal de suivi mal configuré, vous devez supprimer le journal de suivi.

Rubriques

- Trouver vos fichiers CloudTrail journaux
- Téléchargement de vos fichiers CloudTrail journaux

Trouver vos fichiers CloudTrail journaux

CloudTrail publie les fichiers journaux dans votre compartiment S3 dans une archive gzip. Dans le compartiment S3, le fichier journal possède un nom formaté qui comprend les éléments suivants :

- Le nom du bucket que vous avez spécifié lors de la création du trail (disponible sur la page Trails de la CloudTrail console)

- Le préfixe (facultatif) que vous avez spécifié lorsque vous avez créé votre journal d'activité
- La chaîne « AWSLogs »
- Le numéro de compte
- La chaîne « CloudTrail »
- Un identifiant de région tel qu'us-west-1
- L'année de publication du fichier journal au format YYYY
- Le mois de publication du fichier journal au format MM
- Le jour de publication du fichier journal au format DD
- Une chaîne alphanumérique qui lève toute ambiguïté entre le fichier et d'autres qui couvrent la même période

L'exemple suivant montre un nom d'objet fichier journal complet :

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> Pour les traces d'organisation, le nom de l'objet du fichier journal dans le compartiment S3 inclut l'ID de l'unité organisationnelle dans le chemin, comme suit :
>
> ```
> bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

Pour récupérer un fichier journal, vous pouvez utiliser la console Amazon S3, l'interface de ligne de commande (CLI) Amazon S3 ou l'API.

Pour rechercher vos fichiers journaux avec la console Amazon S3

1. Ouvrez la console Amazon S3.
2. Choisissez le compartiment que vous avez spécifié.
3. Parcourez la hiérarchie des objets jusqu'à trouver le fichier journal que vous voulez.

   Tous les fichiers journaux possèdent une extension .gz.

Vous allez parcourir une hiérarchie d'objets qui est similaire à l'exemple suivant, mais avec un nom de compartiment, un ID de compte, une région et une date différents.

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

Un fichier journal pour la hiérarchie des objets précédente ressemble à ce qui suit :

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> Bien que cela arrive rarement, vous pouvez recevoir des fichiers journaux qui contiennent un ou plusieurs événements dupliqués. Dans la plupart des cas, les événements dupliqués auront le même `eventID`. Pour plus d'informations sur le champ `eventID`, consultez la section CloudTrail enregistrer le contenu.

Téléchargement de vos fichiers CloudTrail journaux

Les fichiers journaux sont au format JSON. Si un complément visionneuse JSON est installé, vous pouvez afficher les fichiers directement dans votre navigateur. Double-cliquez sur le nom du fichier journal dans le compartiment pour ouvrir une nouvelle fenêtre ou un nouvel onglet de navigateur. Le code JSON s'affiche alors dans un format lisible.

CloudTrail les fichiers journaux sont des objets Amazon S3. Vous pouvez utiliser la console Amazon S3, la AWS Command Line Interface (CLI) ou l'API Amazon S3 pour récupérer les fichiers journaux.

Pour plus d'informations, consultez la présentation des objets Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

La procédure suivante décrit comment télécharger un fichier journal à l'aide de la AWS Management Console.

Pour télécharger et consulter un fichier journal

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez le compartiment et le fichier journal à télécharger.
3. Choisissez Download (Télécharger) ou Download as (Télécharger sous) et suivez les instructions pour enregistrer le fichier. Le fichier est enregistré dans un format compressé.

   > **Note**
   >
   > Certains navigateurs, tels que Chrome, extraient automatiquement le fichier journal pour vous. Si c'est le cas pour votre navigateur, passez directement à l'étape 5.

4. Utilisez un outil comme 7-Zip pour extraire le fichier journal.
5. Ouvrez le fichier journal dans un éditeur de texte, comme Notepad++.

Pour plus d'informations sur les champs d'événement qui peuvent apparaître dans une entrée de fichier journal, consultez la page CloudTrail enregistrer le contenu.

AWS s'associe à des spécialistes tiers en journalisation et en analyse pour fournir des solutions qui utilisent les CloudTrail résultats. Pour plus d'informations, consultez la section AWS CloudTrail Partenaires.

> **Note**
>
> Vous pouvez également utiliser la fonction Event history (Historique des événements) pour rechercher les événements afin de créer, mettre à jour et supprimer les activités relatives aux API durant les 90 derniers jours.
> Pour de plus amples informations, consultez Utilisation de l'historique des CloudTrail événements.

Configuration des notifications Amazon SNS pour CloudTrail

Vous pouvez être averti lorsque de CloudTrail nouveaux fichiers journaux sont publiés dans votre compartiment Amazon S3. Vous gérez les notifications avec Amazon Simple Notification Service (Amazon SNS).

Les notifications sont facultatives. Si vous souhaitez recevoir des notifications, vous devez configurer CloudTrail pour envoyer des informations de mise à jour à une rubrique Amazon SNS chaque fois qu'un nouveau fichier journal est envoyé. Pour recevoir ces notifications, vous pouvez utiliser Amazon SNS pour vous abonner à la rubrique. En tant qu'abonné, vous pouvez obtenir des mises à jour envoyées à une file d'attente Amazon Simple Queue Service (Amazon SQS), ce qui vous permet de gérer ces notifications par programmation.

Rubriques

Configuration CloudTrail pour envoyer des notifications

Vous pouvez configurer un journal d'activité de sorte qu'il utilise une rubrique Amazon SNS. Vous pouvez utiliser la CloudTrail console ou la commande aws cloudtrail create-trailCLI pour créer le sujet. CloudTrail crée la rubrique Amazon SNS pour vous et y joint une politique appropriée, afin que CloudTrail vous soyez autorisé à publier sur cette rubrique.

Lorsque vous créez un nom de rubrique SNS, celui-ci doit répondre aux critères suivants :

- Contenir 1 à 256 caractères
- Contenir des lettres majuscules et minuscules ASCII, des chiffres, des traits de soulignement ou de traits d'union

Lorsque vous configurez des notifications pour un journal de suivi qui s'applique à toutes les régions, les notifications de toutes les régions sont envoyées à la rubrique Amazon SNS que vous spécifiez. Si vous avez un ou plusieurs journaux de suivi spécifiques à une région, vous devez créer une rubrique distincte pour chaque région et vous abonner à chacune individuellement.

Pour recevoir des notifications, abonnez-vous à la ou aux rubriques Amazon SNS qui CloudTrail utilisent. Pour ce faire, utilisez la console Amazon SNS ou les commandes CLI Amazon SNS. Pour plus d'informations, consultez Abonnement à une rubrique Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

> **Note**
>
> CloudTrail envoie une notification lorsque des fichiers journaux sont écrits dans le compartiment Amazon S3. Un compte actif peut générer un grand nombre de notifications. Si vous vous abonnez par e-mail ou SMS, vous pouvez recevoir un grand volume de messages. Nous vous recommandons de vous abonner avec Amazon Simple Queue Service (Amazon SQS), pour vous permettre de gérer les notifications par programmation. Pour en savoir plus, consultez la section Abonnement d'une file d'attente Amazon SQS à une rubrique Amazon SNS (console) dans le Guide du développeur Amazon Simple Queue Service.

La notification Amazon SNS se compose d'un objet JSON qui comprend un champ `Message`. Le champ `Message` répertorie le chemin d'accès complet au fichier journal, comme illustré dans l'exemple suivant :

```
{
    "s3Bucket": "your-bucket-name","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Si plusieurs fichiers journaux sont transmis au compartiment Amazon S3, une notification peut contenir plusieurs journaux, comme illustré dans l'exemple suivant :

```
{
    "s3Bucket": "your-bucket-name",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

Si vous choisissez de recevoir des notifications par e-mail, le corps de l'e-mail se compose du contenu du champ `Message`. Pour plus d'informations sur la structure JSON, consultez Fanout to Amazon SQS files d'attente dans le manuel Amazon Simple Notification Service Developer Guide. Seul le `Message` champ affiche CloudTrail des informations. Les autres champs contiennent des informations provenant du service Amazon SNS.

Si vous créez un suivi avec l' CloudTrail API, vous pouvez spécifier une rubrique Amazon SNS existante à laquelle vous souhaitez CloudTrail envoyer des notifications avec les opérations `CreateTrail`or `UpdateTrail`. Vous devez vous assurer que le sujet existe et qu'il dispose des autorisations CloudTrail permettant de lui envoyer des notifications. veuillez consulter Politique relative aux rubriques Amazon SNS pour CloudTrail.

Ressources supplémentaires

Pour plus d'informations sur les rubriques Amazon SNS et l'abonnement à celles-ci, consultez le Guide du développeur Amazon Simple Notification Service.

Conseils pour la gestion des journaux d'activité

- À compter du 12 avril 2019, les sentiers ne seront visibles que Régions AWS là où ils enregistrent les événements. Si vous créez un journal qui enregistre tous les événements Régions AWS, il apparaîtra dans la console Régions AWS dans tous les cas de la AWS partition sur laquelle vous travaillez. Si vous créez un journal qui enregistre uniquement les événements dans un seul fichier Région AWS, vous ne pouvez le consulter et le gérer que dans ce cadre Région AWS.
- Pour modifier un journal d'activité de la liste, choisissez son nom.
- Configurez au moins un journal qui s'applique à toutes les régions afin de recevoir les fichiers journaux de toutes les régions de la AWS partition sur laquelle vous travaillez.
- Pour journaliser les événements d'une région spécifique et livrer les fichiers journaux dans un compartiment S3 de la même région, vous pouvez mettre à jour le journal de suivi afin qu'il s'applique à une seule région. Cela est utile si vous souhaitez distinguer vos fichiers journaux. Par exemple, vous souhaiterez peut-être que les utilisateurs gèrent leurs propres journaux dans des régions spécifiques ou que vous souhaitiez séparer les alarmes CloudWatch liées aux journaux par région.
- Pour enregistrer les événements de plusieurs AWS comptes dans un seul journal, pensez à créer une organisation dans, AWS Organizations puis à créer un journal d'organisation.
- La création de plusieurs journaux d'activité entraîne des coûts supplémentaires. Pour en savoir plus sur la tarification, consultez Tarification AWS CloudTrail.

Gestion des coûts des CloudTrail sentiers

À titre de bonne pratique, nous vous recommandons d'utiliser AWS des services et des outils qui peuvent vous aider à gérer CloudTrail les coûts. Vous pouvez également configurer et gérer les CloudTrail traces de manière à capturer les données dont vous avez besoin tout en restant rentable. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Outils permettant de gérer les coûts

AWS Les budgets, une fonctionnalité de AWS Billing and Cost Management, vous permettent de définir des budgets personnalisés qui vous alertent lorsque vos coûts ou votre utilisation dépassent (ou devraient dépasser) le montant budgétisé.

Lorsque vous créez plusieurs pistes, la création d'un budget pour à CloudTrail l'aide de AWS Budgets est une bonne pratique recommandée, qui peut vous aider à suivre vos CloudTrail dépenses. Les budgets basés sur les coûts aident à mieux faire connaître le montant qui pourrait vous être facturé pour votre CloudTrail utilisation. les alertes budgétaires vous avertissent lorsque votre facture atteint un seuil que vous définissez. Lorsque vous recevez une alerte de budget, vous pouvez effectuer des modifications avant la fin du cycle de facturation pour gérer vos coûts.

Après avoir créé un budget, vous pouvez l'utiliser AWS Cost Explorer pour voir comment vos CloudTrail coûts influencent votre AWS facture globale. Dans AWS Cost Explorer, après CloudTrail avoir ajouté le filtre Service, vous pouvez comparer vos CloudTrail dépenses historiques à celles de vos dépenses actuelles month-to-date (MTD), par région et par compte. Cette fonctionnalité vous permet de surveiller et de détecter les coûts imprévus dans vos CloudTrail dépenses mensuelles. Les fonctionnalités supplémentaires de Cost Explorer vous permettent de comparer les CloudTrail dépenses aux dépenses mensuelles au niveau des ressources spécifiques, en fournissant des informations sur les facteurs susceptibles d'entraîner des augmentations ou des baisses de coûts de votre facture.

> **Note**
>
> Bien que vous puissiez appliquer des balises aux CloudTrail sentiers, vous AWS Billing ne pouvez actuellement pas utiliser les balises appliquées aux sentiers pour la répartition des coûts. Cost Explorer peut afficher les coûts des magasins de données sur les événements de CloudTrail Lake et du CloudTrail service dans son ensemble.

Pour commencer à utiliser AWS les budgets, ouvrez AWS Billing and Cost Management, puis choisissez Budgets dans la barre de navigation de gauche. Nous vous recommandons de configurer des alertes budgétaires lorsque vous créez un budget afin de suivre CloudTrail les dépenses. Pour plus d'informations sur l'utilisation des AWS budgets, consultez les sections Gérer vos coûts avec AWS Budgets et Meilleures pratiques pour AWS Budgets.

Configuration d'un journal d'activité

CloudTrail offre de la flexibilité dans la façon dont vous configurez les parcours dans votre compte. Certaines décisions que vous prenez au cours du processus de configuration nécessitent que vous compreniez les impacts sur votre CloudTrail facture. Vous trouverez ci-dessous des exemples de la façon dont la configuration des sentiers peut influencer votre CloudTrail facture.

Création de plusieurs journaux d'activité

Le premier exemplaire des événements de gestion dans chaque région est livré gratuitement. Par exemple, si votre compte comporte deux sentiers dans une seule région, un sentier entrant `us-east-1` et un autre sentier entrant`us-west-2`, aucun CloudTrail frais n'est facturé car il n'y a qu'un seul événement d'enregistrement des sentiers dans chaque région respective. Toutefois, si votre compte comporte un parcours multirégional et un sentier unirégional supplémentaire, le sentier mono-régional entraînera des frais car le sentier multirégional enregistre déjà des événements dans chaque région.

Si vous créez d'autres parcours proposant les mêmes événements de gestion vers d'autres destinations, ces livraisons ultérieures entraînent des CloudTrail coûts. Vous pouvez faire ceci pour autoriser à différents groupes d'utilisateurs (par exemple, les développeurs, le personnel chargé de la sécurité et les auditeurs TI) de recevoir leurs propres copies des fichiers journaux. En ce qui concerne les événements liés aux données, toutes les livraisons entraînent CloudTrail des frais, y compris la première.

En créant des journaux d'activité supplémentaires, il est particulièrement important de vous familiariser avec vos journaux et de comprendre les types et volumes d'événements qui sont générés par des ressources dans votre compte. Cela vous aide à anticiper le volume d'événements associés à un compte et à planifier les coûts liés aux journaux d'activité. Par exemple, l'utilisation du chiffrement côté serveur AWS KMS géré (SSE-KMS) sur vos compartiments S3 peut entraîner l'apparition d'un grand nombre d'événements de gestion. AWS KMS CloudTrail Des volumes d'événements plus importants dans plusieurs journaux d'activité peuvent également avoir un impact sur les coûts.

Pour limiter le nombre d'événements enregistrés dans votre suivi, vous pouvez filtrer les événements de l'API Amazon RDS Data en choisissant Exclure les événements AWS KMS ou Exclure les AWS KMS événements de l'API Amazon RDS Data sur les pages Créer un suivi ou Mettre à jour le suivi. Lorsque vous utilisez des sélecteurs d'événements de base, vous ne pouvez filtrer que les événements de gestion. Vous pouvez toutefois utiliser des sélecteurs d'événements avancés pour filtrer les événements de gestion et de données. Vous pouvez utiliser des sélecteurs d'événements avancés pour inclure ou exclure des événements de données en fonction des champs `resources.type`, `eventName`, `resources.ARN` et `readOnly`, ce qui vous permet de n'enregistrer que les événements de données qui vous intéressent. Pour plus d'informations sur la configuration de ces champs, consultez AdvancedFieldSelector. Pour plus d'informations sur la création et la mise à jour d'un journal de suivi, consultez Création d'un journal de suivi ou Mise à jour d'un journal de suivi dans ce guide.

AWS Organizations

Lorsque vous configurez un suivi des organisations avec CloudTrail, le CloudTrail reproduit sur chaque compte membre de votre organisation. Le nouveau journal d'activité est créé en plus des journaux de suivi existants dans les comptes membres. Assurez-vous que la configuration du journal de suivi de votre organisation correspond à celle des journaux de suivi pour tous les comptes au sein d'une organisation, car la configuration du journal de suivi de l'organisation se propage vers tous les comptes.

Comme Organizations crée un journal de suivi dans chaque compte membre, un compte membre individuel, qui crée un journal de suivi supplémentaire pour collecter les mêmes événements de gestion que le journal de suivi Organizations, collecte une deuxième copie des événements. Cette deuxième copie est facturée au compte. De même, si un compte possède un journal de suivi multi-régions et qu'il crée un deuxième journal de suivi à région unique pour collecter les mêmes événements de gestion que celui multi-régions, le journal de suivi à région unique fournira une deuxième copie des événements. La deuxième copie entraîne des frais.

Consulter aussi

- Tarification AWS CloudTrail
- Gérez vos coûts avec AWS Budgets
- Démarrage avec Cost Explorer
- Se préparer pour la création d'un journal de suivi pour son organisation

Exigences de dénomination

Cette section fournit des informations sur les exigences de dénomination pour les CloudTrail ressources, les compartiments Amazon S3 et les clés KMS.

Rubriques

CloudTrail exigences en matière de dénomination des ressources

CloudTrail les noms de ressources doivent répondre aux exigences suivantes :

- Contenir uniquement des lettres ASCII (a à z, A à Z), des chiffres (0 à 9), des points (.) et des traits de soulignement (_) ou des tirets (-).
- Démarrer par une lettre ou un nombre et terminer par une lettre ou un nombre.
- Contenir entre 3 et 128 caractères.
- N'avoir aucun point, trait de soulignement ou tiret adjacent. Des noms comme my-_namespace et my-\-namespace ne sont pas valides.
- Ne pas être au format d'adresse IP (par exemple, `192.168.5.4`).

Conditions d'attribution de noms pour des compartiments Amazon S3.

Le compartiment Amazon S3 que vous utilisez pour stocker les fichiers CloudTrail journaux doit avoir un nom conforme aux exigences de dénomination pour les régions non conformes aux normes américaines. Amazon S3 définit un nom de compartiment comme une série d'une ou plusieurs étiquettes, séparées par des points. Pour obtenir la liste complète des règles de dénomination, veuillez consulter Règles de dénomination des compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

Voici quelques-unes des règles :

- Le nom du compartiment peut compter entre 3 et 63 caractères et contenir uniquement des caractères minuscules, des chiffres, des points et des tirets.

- Chaque étiquette dans le nom de compartiment doit commencer par une lettre minuscule ou un chiffre.
- Le nom de compartiment ne peut pas contenir de traits de soulignement, terminer par un tiret, avoir plusieurs points consécutives ou des tirets à côté de points.
- Le nom de compartiment ne doit pas utiliser le même format qu'une adresse IP (198.51.100.24).

> **Warning**
>
> Etant donné que S3 autorise votre compartiment d'être utilisé comme une URL qui accessible publiquement, le nom de compartiment que vous choisissez doit être globalement unique. Si un autre compte a déjà créé un compartiment avec le nom que vous avez choisi, vous devez utiliser un autre nom. Pour de plus amples informations, consultez Limites et restrictions applicables aux compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

AWS KMS exigences relatives à la dénomination des alias

Lorsque vous créez un AWS KMS key, vous pouvez choisir un alias pour l'identifier. Par exemple, vous pouvez choisir l'alias « KMS- CloudTrail -us-west-2 » pour chiffrer les journaux d'un parcours spécifique.

L'alias doit répondre aux critères suivants :

- Entre 1 et 256 caractères, inclus
- Contenir des caractères alphanumériques (A-Z, a-z, 0-9), des tirets (-), des barres obliques (/) et des traits de soulignement (_)
- Ne doit pas commencer par aws

Pour en savoir plus, consultez Création des clés dans le Guide du développeur AWS Key Management Service .

Créer plusieurs journaux d'activité

Vous pouvez utiliser les fichiers CloudTrail journaux pour résoudre les problèmes opérationnels ou de sécurité de votre AWS compte. Vous pouvez créer des journaux d'activité pour différents utilisateurs, qui eux-mêmes peuvent créer et gérer leurs propres journaux d'activité. Vous pouvez configurer les

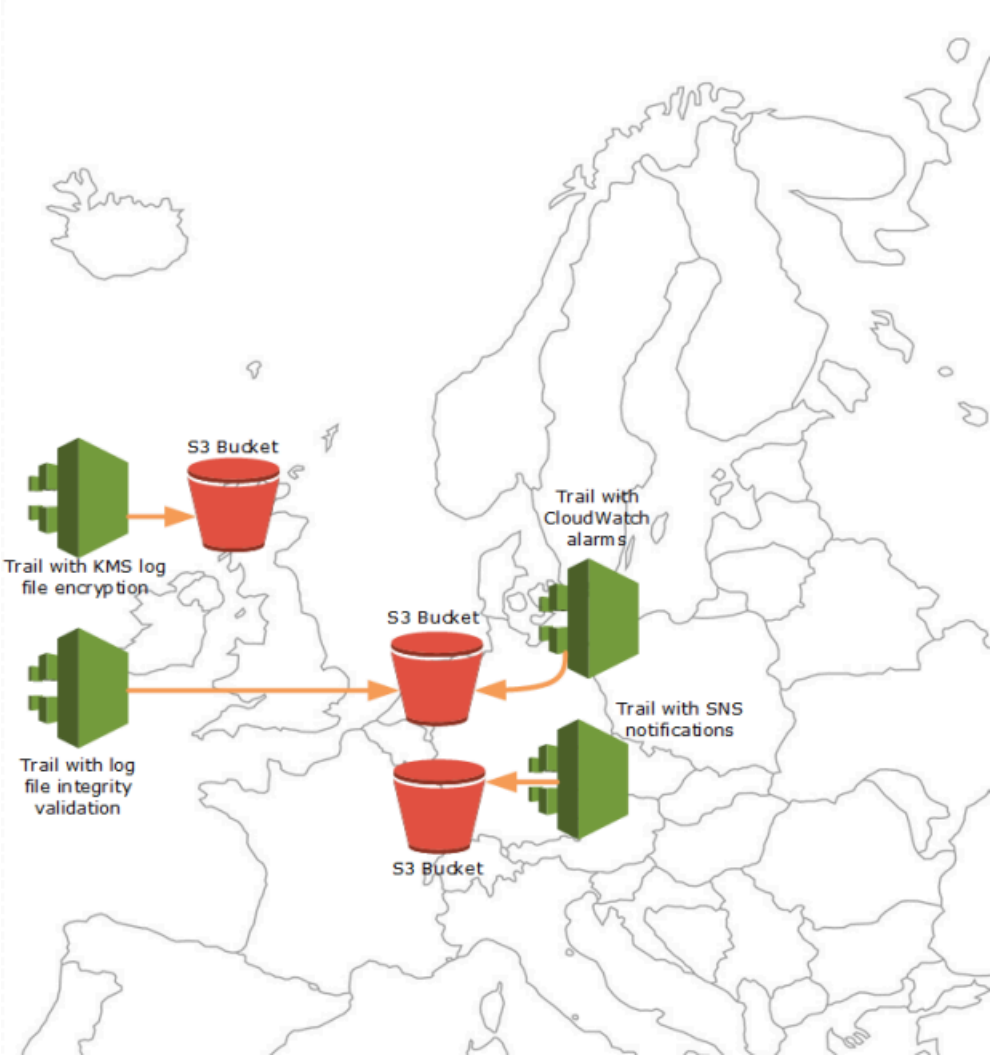
journaux d'activité de manière à livrer les fichiers journaux dans des compartiments S3 séparés ou partagés.

> **Note**
>
> La première copie des événements de gestion Région AWS de chaque compte est gratuite. Si vous créez d'autres parcours proposant les mêmes événements de gestion vers d'autres destinations, ces livraisons ultérieures entraînent des CloudTrail coûts. Pour plus d'informations sur CloudTrail les coûts, consultez la section AWS CloudTrail Tarification etGestion des coûts des CloudTrail sentiers.

Par exemple, vous pouvez avoir les utilisateurs suivants :

- Un administrateur de sécurité crée un journal d'activité dans la Région Europe (Irlande) et configure le chiffrement des fichiers journaux KMS. Le journal d'activité livre les fichiers journaux dans un compartiment S3 dans la Région Europe (Irlande).
- Un auditeur informatique crée une trace dans la région Europe (Irlande) et configure la validation de l'intégrité des fichiers journaux pour s'assurer que les fichiers journaux n'ont pas changé depuis leur CloudTrail livraison. Le journal d'activité est configuré pour livrer les fichiers journaux dans un compartiment S3 dans la Région Europe (Francfort)
- Un développeur crée un parcours dans la région Europe (Francfort) et configure les CloudWatch alarmes pour recevoir des notifications relatives à une activité d'API spécifique. Le journal d'activité partage le même compartiment S3 que le journal d'activité configuré pour l'intégrité des fichiers journaux.
- Un autre développeur crée un journal d'activité dans la Région Europe (Francfort) et configure SNS. Les fichiers journaux sont livrés dans un compartiment S3 distinct dans la Région Europe (Francfort).

L'image suivante illustre cet exemple.



> **Note**
>
> Vous pouvez créer jusqu'à cinq sentiers par Région AWS. Un sentier multirégional compte pour un sentier par région.

Vous pouvez utiliser les autorisations au niveau des ressources pour gérer la capacité d'un utilisateur à effectuer des opérations spécifiques sur. CloudTrail

Par exemple, vous pouvez accorder à un utilisateur l'autorisation d'afficher l'activité du journal d'activité, mais empêcher l'utilisateur de démarrer ou d'arrêter la journalisation pour un journal d'activité. Vous pouvez accorder à un autre utilisateur des autorisations complètes de création et de suppression de journaux d'activité. Cela vous permet un meilleur contrôle de vos journaux d'activité et des accès utilisateur.

Pour plus d'informations sur les autorisations au niveau des ressources, consultez Exemples : créer et appliquer des politiques pour des actions sur des journaux de suivi spécifiques.

Pour plus d'informations sur les sentiers multiples, consultez les CloudTrail FAQ.

Contrôle des autorisations des utilisateurs pour les CloudTrail sentiers

AWS CloudTrail s'intègre à AWS Identity and Access Management (IAM) pour vous aider à contrôler l'accès aux ressources requises CloudTrail et aux autres AWS ressources qui en ont CloudTrail besoin. Les compartiments Amazon S3 et les rubriques Amazon Simple Notification Service (Amazon SNS) sont des exemples de ces ressources. Vous pouvez utiliser IAM pour contrôler quels AWS utilisateurs peuvent créer, configurer ou supprimer des CloudTrail traces, démarrer et arrêter la journalisation, et accéder aux compartiments contenant les informations des journaux. Pour en savoir plus, veuillez consulter la section Identity and Access Management pour AWS CloudTrail.

Les rubriques suivantes vous aident à comprendre les autorisations, les politiques et CloudTrail la sécurité :

- Octroi d'autorisations pour CloudTrail l'administration
- Règles de dénomination de compartiment Amazon S3
- Politique relative aux compartiments Amazon S3 pour CloudTrail
- Voici un exemple de stratégie de compartiment pour un journal d'activité d'une organisation dans Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface.
- Politique relative aux rubriques Amazon SNS pour CloudTrail
- Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS)
- Autorisations requises pour copier les événements de journal de suivi
- Autorisations requises pour attribuer un administrateur délégué
- Politique de clé KMS par défaut créée dans CloudTrail la console
- Octroi de l'autorisation AWS Config d'afficher les informations sur la CloudTrail console
- Partage de fichiers CloudTrail journaux entre AWS comptes
- Autorisations requises pour créer un journal de suivi d'organisation
- Utilisation d'un rôle IAM existant pour ajouter la surveillance du suivi d'une organisation à Amazon Logs CloudWatch

Utilisation AWS CloudTrail avec les points de terminaison VPC de l'interface

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez établir une connexion privée entre votre VPC et. AWS CloudTrail Vous pouvez utiliser cette connexion pour CloudTrail communiquer avec vos ressources sur votre VPC sans passer par l'Internet public.

Amazon VPC est un AWS service que vous pouvez utiliser pour lancer AWS des ressources dans un réseau virtuel que vous définissez. Avec un VPC, vous contrôlez des paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau. Avec les points de terminaison VPC, le routage entre le VPC et les AWS services est géré par le AWS réseau, et vous pouvez utiliser les politiques IAM pour contrôler l'accès aux ressources des services.

Pour connecter votre VPC à CloudTrail, vous définissez un point de terminaison VPC d'interface pour. CloudTrail Un point de terminaison d'interface est une interface elastic network dotée d'une adresse IP privée qui sert de point d'entrée pour le trafic destiné à un AWS service pris en charge. Le point de terminaison fournit une connectivité fiable et évolutive CloudTrail sans nécessiter de passerelle Internet, d'instance de traduction d'adresses réseau (NAT) ou de connexion VPN. Pour de plus amples informations, consultez Qu'est-ce qu'Amazon VPC ? dans le Guide de l'utilisateur Amazon VPC.

Les points de terminaison VPC d'interface sont alimentés par AWS PrivateLink une AWS technologie qui permet une communication privée entre les AWS services à l'aide d'une interface Elastic Network avec des adresses IP privées. Pour plus d'informations, consultez AWS PrivateLink.

Les étapes suivantes s'adressent aux utilisateurs d'Amazon VPC. Pour plus d'informations, consultez Mise en route avec Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

Disponibilité

CloudTrail prend actuellement en charge les points de terminaison VPC dans les régions suivantes : AWS

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)

- USA Ouest (Oregon)
- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Osaka)
- Asia Pacific (Seoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Canada Ouest (Calgary)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Milan)
- Europe (Paris)
- Europe (Espagne)
- Europe (Stockholm)
- Europe (Zurich)
- Israël (Tel Aviv)
- Moyen-Orient (Bahreïn)
- Moyen-Orient (EAU)
- Amérique du Sud (São Paulo)
- AWS GovCloud (USA Est)
- AWS GovCloud (US-Ouest)

Créez un point de terminaison VPC pour CloudTrail

Pour commencer à utiliser CloudTrail avec votre VPC, créez un point de terminaison VPC d'interface pour. CloudTrail Pour plus d'informations, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Il n'est pas nécessaire de modifier les paramètres de CloudTrail. CloudTrail appelle d'autres utilisateurs Services AWS en utilisant des points de terminaison publics ou des points de terminaison VPC d'interface privée, selon ceux utilisés.

Sous-réseaux partagés

Un point de terminaison CloudTrail VPC, comme tout autre point de terminaison VPC, ne peut être créé que par un compte propriétaire dans le sous-réseau partagé. Toutefois, un compte de participant peut utiliser des points de terminaison CloudTrail VPC dans des sous-réseaux partagés avec le compte de participant. Pour plus d'informations sur le partage de sous-réseaux Amazon VPC, veuillez consulter Partager votre VPC avec d'autres comptes dans le Guide de l'utilisateur Amazon VPC.

Compte AWS fermeture et sentiers

AWS CloudTrail surveille et enregistre en permanence les événements relatifs à l'activité du compte générés par un utilisateur, un rôle ou Service AWS pour un Compte AWS. Les utilisateurs peuvent créer un CloudTrail journal pour recevoir une copie de ces événements dans un compartiment S3 dont ils sont propriétaires.

CloudTrail est un service de sécurité fondamental. Par conséquent, les sentiers créés par les utilisateurs continuent d'exister et de générer des événements même après leur fermeture, à moins qu'un utilisateur ne supprime explicitement les sentiers qu'ils contiennent Compte AWS avant de les fermer. Compte AWS Ce comportement s'applique également aux journaux de suivi d'organisation crées par le compte de gestion ou par l'administrateur délégué, ainsi qu'aux journaux de suivi d'organisation multi-Régions qui sont ensuite créés dans les comptes des membres de l'organisation. Cela garantit que si un utilisateur rouvre un compte fermé, il dispose d'un historique ininterrompu de l'activité du compte. Il fournit également aux utilisateurs une visibilité sur toute activité finale du compte, y compris la suppression et la résiliation des ressources et services restants du compte.

Les utilisateurs ont la possibilité de supprimer les pistes avant de les fermer ou de les contacter AWS Supportpour demander la suppression des pistes après leur Compte AWS fermeture. Compte AWS

Pour plus d'informations sur la fermeture d'un Compte AWS, voir Fermer un Compte AWS.

> **Note**
>
> Si la validation des fichiers CloudTrail journaux est activée, les utilisateurs continueront de recevoir des fichiers résumés horaires indiquant si des CloudTrail journaux ont été créés ou non.
>
> CloudTrail Les magasins de données sur les événements CloudTrail Lake, les canaux Lake pour les intégrations, les canaux CloudTrail liés aux services et les ressources créées pour les traces (par exemple, les groupes de CloudWatch journaux Amazon Logs et les compartiments Amazon S3 présents dans le compte fermé) suivent le AWS comportement standard en matière de fermeture de compte et sont définitivement supprimés après la période post-fermeture (généralement 90 jours).

Configurer les CloudTrail paramètres

Vous pouvez utiliser la page Paramètres de la CloudTrail console pour configurer et vérifier CloudTrail les paramètres.

Pour accéder à la page des paramètres

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Choisissez Paramètres dans le volet de navigation de gauche de la CloudTrail console.
3. Vérifiez et mettez à jour vos paramètres selon vos besoins.

   Les paramètres suivants sont disponibles :

   - Administrateurs délégués de l'organisation : si vous avez une AWS Organizations organisation, vous pouvez afficher les administrateurs CloudTrail délégués, ajouter des administrateurs délégués (jusqu'à trois au maximum) et supprimer des administrateurs délégués. Seul le compte de gestion de l'organisation peut ajouter ou supprimer des administrateurs délégués.

     Le compte de gestion de l'organisation peut affecter n'importe quel compte au sein de l'organisation pour agir en tant qu'administrateur CloudTrail délégué chargé de gérer les sentiers et les magasins de données sur les événements de l'organisation pour le compte de l'organisation.
   - Canaux liés à un service— Vous pouvez consulter toutes les chaînes liées au service créées pour votre compte.

     Services AWS peut créer un canal lié à un service pour recevoir des CloudTrail événements en votre nom. Le AWS service qui crée le canal lié au service configure les sélecteurs d'événements avancés pour le canal et indique si le canal s'applique à tous ou à un seul Régions AWS. Région AWS

Administrateur délégué de l'organisation

Lorsque vous l'utilisez CloudTrail avec une AWS Organizations organisation, vous pouvez attribuer à n'importe quel compte au sein de l'organisation le rôle d'administrateur CloudTrail délégué chargé de gérer les traces et les banques de données d'événements de l'organisation pour le compte

de l'organisation. Un administrateur délégué est un compte membre d'une organisation qui peut effectuer les mêmes tâches administratives (sauf indication contraire) CloudTrail que le compte de gestion.

Si vous choisissez un administrateur délégué, ce compte membre dispose d'autorisations administratives sur tous les journaux de suivi et entrepôts de données d'événement d'organisation. L'ajout d'un administrateur délégué ne modifie pas la gestion ou le fonctionnement des journaux de suivi ou des entrepôts de données d'événement de l'organisation.

La première fois que vous ajoutez un administrateur délégué dans la CloudTrail console, ou à l'aide de l' CloudTrail API AWS CLI or, vérifiez si CloudTrail le compte de gestion de l'organisation possède un rôle lié à un service. Si le compte de gestion n'a pas de rôle lié à un service, CloudTrail crée le rôle lié au service pour le compte de gestion. Pour plus d'informations sur les rôles liés à un service, consultez Utilisation de rôles liés à un service pour AWS CloudTrail.

> **Note**
>
> Lorsque vous ajoutez un administrateur délégué à l'aide de la AWS Organizations CLI ou de l'API, le rôle lié au service n'est pas créé s'il n'existe pas. Le rôle lié au service n'est créé que lorsque vous passez un appel directement au CloudTrail service depuis le compte de gestion, par exemple lorsque vous ajoutez un administrateur délégué ou que vous créez un journal d'organisation ou un magasin de données d'événements à l'aide de la CloudTrail console AWS CLI ou CloudTrail de l'API.

Prenez note des facteurs suivants qui définissent le mode de fonctionnement de l'administrateur délégué CloudTrail.

Le compte de gestion reste propriétaire de toutes les ressources de CloudTrail l'organisation créées par l'administrateur délégué.

Le compte de gestion de l'organisation reste propriétaire de toutes les ressources de CloudTrail l'organisation créées par l'administrateur délégué, telles que les sentiers et les magasins de données sur les événements. Cela assure la continuité de l'organisation en cas de changement d'administrateur délégué.

La suppression d'un compte d'administrateur délégué ne supprime aucune des ressources d' CloudTrail organisation qu'il a créées.

> Les traces d'organisation et les banques de données d'événements créées par l'administrateur délégué ne sont pas supprimées lorsque vous supprimez l'administrateur délégué, car le compte de gestion est toujours le propriétaire des ressources de CloudTrail l'organisation, qu'elles soient créées par l'administrateur délégué ou par le compte de gestion.

Une organisation peut avoir un maximum de trois administrateurs CloudTrail délégués.

> Vous pouvez avoir un maximum de trois administrateurs CloudTrail délégués par organisation. Pour plus d'informations sur la suppression d'un compte administrateur délégué, consultez Supprimer un administrateur CloudTrail délégué.

Le tableau suivant présente les fonctionnalités du compte de gestion, des comptes d'administrateur délégué et des comptes membres de l' AWS Organizations organisation.

Fonctionnalités	Compte de gestion	Compte administrateur délégué	Comptes membres
Ajouter ou supprimer des comptes administrateur délégué.	Oui	Non	Non
Créer un journal de suivi d'organisation.	Oui	Oui[1]	Non
Afficher une liste des journaux de suivi d'organisation.	Oui	Oui	Oui
Mettre à jour un journal de suivi d'organisation.	Oui	Oui[1, 2]	Non
Supprimer un journal de suivi d'organisation.	Oui	Oui	Non
Créez un magasin de données d'événements d'organisation pour les CloudTrail événements ou les	Oui	Oui	Non

Fonctionnalités	Compte de gestion	Compte administrateur délégué	Comptes membres
éléments AWS Config de configura tion.			
Activer Insights sur le magasin de données d'événement d'organisation.	Oui	Non	Non
Mettre à jour un magasin de données d'événement d'organisation.	Oui	Oui[2]	Non
Activer la fédération de requêtes Lake sur un magasin de données d'événement d'organisation[3].	Oui	Oui	Non
Désactiver la fédération de requêtes Lake dans un magasin de données d'événement d'organisation.	Oui	Oui	Non
Supprimer un magasin de données d'événement d'organisation.	Oui	Oui	Non
Copier des événements de journal de suivi dans un magasin de données d'événement d'organisation.	Oui	Non	Non
Exécuter des requêtes sur des magasins de données d'événement d'organisation.	Oui	Oui	Non
Afficher le tableau de bord Lake d'un magasin de données d'événement d'organisation.	Oui	Oui	Non

[1] L'administrateur délégué peut uniquement configurer un groupe de CloudWatch journaux Logs à l'aide des opérations AWS CLI CloudTrail `CreateTrail` ou de `UpdateTrail` l'API. Le groupe de CloudWatch journaux et le rôle de journal doivent tous deux exister dans le compte appelant.

[2] Seul le compte de gestion peut convertir un magasin de données de suivi ou d'événement d'une organisation en un magasin de données de suivi ou d'événement au niveau du compte, ou convertir un magasin de données de suivi ou d'événement au niveau du compte en un journal d'organisation ou un magasin de données d'événements. Ces actions ne sont pas autorisées pour l'administrateur délégué, car les journaux de suivi et les entrepôts de données d'événements d'organisation n'existent que dans le compte de gestion. Lorsqu'un magasin de données de suivi ou d'événement d'une organisation est converti en un magasin de données de suivi ou d'événement au niveau du compte, seul le compte de gestion a accès au magasin de données de suivi ou d'événement.

[3]Un seul compte administrateur délégué ou le compte de gestion peut activer la fédération dans le magasin de données d'événement d'organisation. D'autres comptes administrateur délégué peuvent interroger et partager des informations à l'aide de la fonctionnalité de partage de données de Lake Formation. Tout compte administrateur délégué ainsi que le compte de gestion de l'organisation peuvent désactiver la fédération.

Rubriques

Autorisations requises pour attribuer un administrateur délégué

Lorsque vous affectez un administrateur CloudTrail délégué, vous devez disposer des autorisations nécessaires pour ajouter et supprimer l'administrateur délégué CloudTrail, ainsi que certaines actions d' AWS Organizations API et autorisations IAM répertoriées dans la déclaration de politique suivante.

Vous pouvez ajouter l'instruction suivante à la fin d'une politique IAM existante pour accorder ces autorisations :

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
```

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

Ajouter un administrateur CloudTrail délégué

Vous pouvez ajouter un administrateur délégué pour gérer les CloudTrail ressources d'une organisation, telles que les sentiers et les magasins de données sur les événements.

Vous pouvez ajouter un administrateur CloudTrail délégué pour votre AWS organisation à l'aide de la CloudTrail console ou du AWS CLI.

Avant d'ajouter un administrateur délégué, assurez-vous qu'il possède un compte dans votre organisation et que vous êtes connecté avec le compte de gestion de votre organisation. Pour plus d'informations sur la création d'un nouveau AWS compte pour votre organisation, consultez la section Création d'un AWS compte dans votre organisation. Pour plus d'informations sur la façon d'inviter un AWS compte existant dans votre organisation, voir Inviter un AWS compte à rejoindre votre organisation.

CloudTrail console

La procédure suivante explique comment ajouter un administrateur CloudTrail délégué à l'aide de la CloudTrail console.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Choisissez Paramètres dans le volet de navigation de gauche de la CloudTrail console.
3. Dans la section Organization delegated administrators (Administrateurs délégués de l'organisation), choisissez Register administrator (Enregistrer l'administrateur).
4. Entrez l'identifiant de AWS compte à douze chiffres du compte que vous souhaitez attribuer en tant qu'administrateur CloudTrail délégué pour les magasins de données sur les sentiers et les événements de l'organisation.
5. Sélectionnez Register administrator (Enregistrer l'administrateur).

AWS CLI

L'exemple suivant ajoute un administrateur CloudTrail délégué.

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

Cette commande ne produit aucune sortie si elle réussit.

Supprimer un administrateur CloudTrail délégué

Vous pouvez supprimer un administrateur CloudTrail délégué à l'aide de la CloudTrail console ou du AWS CLI.

CloudTrail console

La procédure suivante explique comment supprimer un administrateur CloudTrail délégué à l'aide de la CloudTrail console.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Choisissez Paramètres dans le volet de navigation de gauche de la CloudTrail console.
3. Dans la section Organization delegated administrators (Administrateurs délégués de l'organisation), choisissez l'administrateur délégué que vous souhaitez supprimer.
4. Choisissez Remove administrator (Supprimer l'administrateur).
5. Confirmez que vous souhaitez supprimer l'administrateur délégué, puis choisissez Remove administrator (Supprimer l'administrateur).

AWS CLI

La commande suivante supprime un administrateur CloudTrail délégué.

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

Cette commande ne produit aucune sortie si elle réussit.

Canaux liés à un service

AWS les services peuvent créer un canal lié à un service pour recevoir des CloudTrail événements en votre nom. Le AWS service qui crée le canal lié au service configure les sélecteurs d'événements

avancés pour le canal et indique si le canal s'applique à tous ou à un seul Régions AWS. Région AWS

Rubriques

Afficher les canaux liés aux services à l'aide de la console

À l'aide de la CloudTrail console, vous pouvez consulter les informations relatives à tous les canaux CloudTrail liés aux services créés par AWS les services. Le tableau est vide si votre compte ne comporte aucun canal lié à un service.

Utilisez la procédure suivante pour afficher les informations relatives à un canal lié à un service.

1. Choisissez Paramètres dans le volet de navigation de gauche de la CloudTrail console.
2. Dans Canaux liés aux services, choisissez un canal lié au service pour en afficher les détails.
3. Sur la page de détails, passez en revue les paramètres configurés du canal lié à un service.

   Vous pouvez consulter les informations suivantes sur la page de détails.

   - Nom du canal : nom complet du canal. Le format du nom du canal correspond à l'`aws-service-channel/`*`AWS_service_name`*`/slc`endroit où *`AWS_service_name`* représente le nom du AWS service qui gère le canal.
   - ARN du canal : ARN du canal, que vous pouvez utiliser dans une demande d'API pour obtenir des informations sur le canal.
   - Toutes les régions : la valeur est `Yes` si le canal est configuré pour toutes les Régions AWS.
   - AWS service : nom du AWS service qui gère le canal.
   - Événements de gestion : affiche tous les événements de gestion configurés pour le canal.
   - Événements de données : affiche tous les événements de données configurés pour le canal.

Afficher les chaînes liées au service à l'aide du AWS CLI

À l'aide du AWS CLI, vous pouvez afficher des informations sur tous les canaux CloudTrail liés aux services créés par AWS les services.

Rubriques

- Accédez à un canal lié à un CloudTrail service
- Répertorier tous les CloudTrail canaux liés au service
- AWS événements de service sur les canaux liés aux services

Accédez à un canal lié à un CloudTrail service

L'exemple de AWS CLI commande suivant renvoie des informations sur un canal CloudTrail lié à un service spécifique, notamment le nom du AWS service de destination, les sélecteurs avancés configurés pour le canal et si le canal s'applique à toutes les régions ou à une seule région.

Vous devez spécifier un ARN ou le suffixe d'ID d'un ARN pour `--channel`.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

Voici un exemple de réponse. Dans cet exemple, `AWS_service_name` représente le nom du AWS service qui a créé le canal.

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
                        ]
                    }
                ]
            }
        ]
    },
```

```
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
    ]
}
```

Répertorier tous les CloudTrail canaux liés au service

L'exemple de AWS CLI commande suivant renvoie des informations sur tous les canaux CloudTrail liés au service qui ont été créés en votre nom. Les paramètres facultatifs incluent `--max-results`, pour spécifier un nombre maximal de résultats que la commande doit renvoyer sur une seule page. S'il y a plus de résultats que la valeur `--max-results` spécifiée, exécutez à nouveau la commande en ajoutant la valeur `NextToken` renvoyée pour obtenir la page suivante de résultats.

```
aws cloudtrail list-channels
```

Voici un exemple de réponse. Dans cet exemple, `AWS_service_name` représente le nom du AWS service qui a créé le canal.

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS événements de service sur les canaux liés aux services

Le AWS service qui gère le canal lié au service peut lancer des actions sur le canal lié au service (par exemple, créer ou mettre à jour un canal lié au service). CloudTrail enregistre ces actions en tant qu'événements de AWS service et enregistre ces événements dans l'historique des événements, ainsi que dans les traces actives et les banques de données d'événements configurées pour les événements de gestion. Pour ces événements, le champ `eventType` est `AwsServiceEvent`.

Voici un exemple d'entrée dans un fichier journal d'un événement de AWS service pour la création d'un canal lié à un service.


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
   "eventSource":"cloudtrail.amazonaws.com",
   "eventName":"CreateServiceLinkedChannel",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"AWS Internal",
   "requestParameters":null,
   "responseElements":null,
   "requestID":"564f004c-EXAMPLE",
   "eventID":"234f004b-EXAMPLE",
   "readOnly":false,
   "resources":[
      {
         "accountId":"184434908391",
         "type":"AWS::CloudTrail::Channel",
         "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
      }
   ],
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "recipientAccountId":"111122223333",
   "eventCategory":"Management"
}
```

Comprendre les CloudTrail événements

Un événement dans CloudTrail est l'enregistrement d'une activité sur un AWS compte. Cette activité peut être une action entreprise par une identité IAM ou un service contrôlable par. CloudTrail CloudTrail les événements fournissent un historique de l'activité des comptes API et non-API effectuée via les AWS SDK AWS Management Console, les outils de ligne de commande, etc. Services AWS

CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

Il existe trois types d' CloudTrail événements :

- Événements de gestion
- Événements de données
- Événements Insights

Par défaut, les journaux de suivi et les entrepôts de données d'événement consignent les événements de gestion, mais pas les événements de données ou les événements Insights.

Tous les types d'événements utilisent un format de journal CloudTrail JSON. Le journal contient des informations sur les demandes pour les ressources de votre compte, telles que l'auteur de la demande, les services utilisés, les actions réalisées et les paramètres pour l'action. Les données d'événement sont contenues dans un tableau `Records`.

Pour plus d'informations sur les champs d'enregistrement d' CloudTrail événements, consultezCloudTrail enregistrer le contenu.

Événements de gestion

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom opérations de plan de contrôle. Les événements de gestion sont notamment les suivants :

- Configuration de la sécurité (par exemple, les opérations d' AWS Identity and Access Management `AttachRolePolicy`API).
- Enregistrement des appareils (par exemple, les opérations d'API `CreateDefaultVpc` Amazon EC2).

- Configuration des règles de routage des données (par exemple, les opérations d'API `CreateSubnet` Amazon EC2).
- Configuration de la journalisation (par exemple, les opérations d' AWS CloudTrail `CreateTrail`API).

Les événements de gestion peuvent aussi inclure les événements non API qui se produisent dans votre compte. Par exemple, lorsqu'un utilisateur se connecte à votre compte, CloudTrail enregistre l'`ConsoleLogin`événement. Pour plus d'informations, consultez Événements non liés à l'API capturés par CloudTrail. Pour obtenir la liste des événements de gestion qui CloudTrail enregistrent les AWS services, consultezCloudTrail services et intégrations pris en charge.

L'exemple suivant montre un enregistrement de journal unique d'un événement de gestion. Dans cet événement, un utilisateur IAM nommé `Mary_Major` a exécuté la aws cloudtrail start-logging commande pour lancer CloudTrail `StartLogging`le processus de journalisation sur une piste nomméemy`Trail`.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
        "name": "myTrail"
```

```
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Dans l'exemple suivant, un utilisateur IAM nommé `Paulo_Santos` a exécuté la commande aws cloudtrail start-event-data-store-ingestion pour appeler l'action `StartEventDataStoreIngestion` permettant de démarrer l'ingestion dans un entrepôt de données d'événement.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


Événements de données

Les événements de données fournissent des informations sur les opérations de ressource exécutées sur ou dans une ressource. Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé.

Les événements de données incluent notamment :

- Activité de l'API au niveau des objets Amazon S3 (par exemple, `GetObject`, `DeleteObject`, et opérations d'`PutObject`API) sur des objets dans des compartiments S3.
- AWS Lambda activité d'exécution de fonctions (l'`Invoke`API).
- CloudTrail `PutAuditEvents`activité sur un chenal CloudTrail lacustre utilisé pour enregistrer des événements provenant de l'extérieur AWS.
- Opérations d'API `Publish` et `PublishBatch` d'Amazon SNS sur des rubriques.

Le tableau suivant indique les types d'événements de données disponibles pour les journaux de suivi et les entrepôts de données d'événement. La colonne Type d'événement de données (console)

indique la sélection appropriée dans la console. La colonne de valeur resources.type indique la `resources.type` valeur que vous devez spécifier pour inclure les événements de données de ce type dans votre magasin de données de suivi ou d'événement à l' AWS CLI aide des API or. CloudTrail

Pour les traces, vous pouvez utiliser des sélecteurs d'événements de base ou avancés pour enregistrer les événements de données relatifs aux objets Amazon S3, aux fonctions Lambda et aux tables DynamoDB (illustrés dans les trois premières lignes du tableau). Vous ne pouvez utiliser que des sélecteurs d'événements avancés pour enregistrer les types d'événements de données indiqués dans les lignes restantes.

Pour les entrepôts de données d'événement, vous ne pouvez utiliser que des sélecteurs d'événements avancés pour inclure les événements de données.

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon DynamoDB	Activité de l'API au niveau des éléments Amazon DynamoDB sur les tables (par exemple `PutItem`, `DeleteItem`, et les opérations d'API). `UpdateItem` **Note** Pour les tables ayant les flux activés, le champ `resources` dans l'événement de données	DynamoDB	`AWS::DynamoDB::Table`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.		

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS Lambda	AWS Lambda activité d'exécution de fonctions (l'`Invoke`API).	Lambda	`AWS::Lambda::Function`
Amazon S3	Activité de l'API au niveau des objets Amazon S3 (par exemple, `GetObject` `DeleteObject` , et opérations d'`PutObject` API) sur des objets dans des compartiments S3.	S3	`AWS::S3::Object`
AWS AppConfig	AWS AppConfig Activité de l'API pour les opérations de configuration telles que les appels vers `StartConfiguration` `SessionetGetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS Échange de données B2B	Activité de l'API d'échange de données B2B pour les opérations du transformateur telles que les appels vers `GetTransformerJob` et `StartTransformerJob` .	Échange de données B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Activité de l'API Amazon Bedrock sur un alias d'agent.	Alias d'agent Bedrock	`AWS::Bedrock::AgentAlias`
	Activité de l'API Amazon Bedrock sur une base de connaissances.	Base de connaissances Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront Activité de l'API sur un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Activité de l'API sur un espace de noms.	AWS Cloud Map espace de nom	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Activité de l'API sur un service.	AWS Cloud Map web	`AWS::ServiceDiscovery::Service`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS CloudTrail	CloudTrail `PutAuditEvents` activité sur un chenal CloudTrail lacustre utilisé pour enregistrer des événements provenant de l'extérieur AWS.	CloudTrail canal	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Activité de CodeWhisperer l'API Amazon sur une personnalisation.	CodeWhisperer personnalisation	`AWS::CodeWhisperer::Customization`
	Activité de CodeWhisperer l'API Amazon sur un profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Activité de l'API Amazon Cognito sur les réserves d'identités Amazon Cognito.	Réserves d'identités Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Activité de l'API Amazon DynamoDB sur les flux.	DynamoDB Streams	`AWS::DynamoDB::Stream`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Elastic Block Store	API directes Amazon Elastic Block Store (EBS) telles que `PutSnapshotBlock`, `GetSnapshotBlock`, et `ListChangedBlocks` sur des instantanés Amazon EBS.	API directes Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Activité de l'API Amazon EMR sur un espace de travail de journalisation à écriture anticipée.	Espace de travail de journalisation à écriture anticipée EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Activité de l'API Amazon FinSpace sur les environnements.	FinSpace	`AWS::FinSpace::Environment`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS Glue	AWS Glue Activité de l'API sur les tables créées par Lake Formation. **Note** AWS Glue les événements de données pour les tables ne sont actuellement pris en charge que dans les régions suivantes : • USA Est (Virginie du Nord) • USA Est (Ohio) • USA Ouest (Oregon) • Europe (Irlande) • Région Asie-	Lake Formation	`AWS::Glue::Table`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Pacifique (Tokyo)		
Amazon GuardDuty	Activité de GuardDuty l'API Amazon pour un détecteur.	GuardDuty détecteur	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Activité de l'API sur les magasins de données.	Magasin de données d'imagerie médicale	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Activité de l'API sur les certificats.	Certificat IoT	`AWS::IoT::Certificate`
	AWS IoT Activité de l'API sur les objets.	Un truc lié à l'IoT	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	Activité de l'API Greengrass depuis un appareil principal de Greengrass sur une version de composant . **Note** Greengrass n'enregistre pas les cas de refus d'accès.	Version du composant IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de l'API Greengrass depuis un appareil principal de Greengrass lors d'un déploiement. **Note** Greengrass n'enregistre pas les cas de refus d'accès.	Déploiement de Greengrass pour l'IoT	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Activité de SiteWise l'API IoT sur les actifs.	SiteWise Actif IoT	`AWS::IoTSiteWise::Asset`
	Activité de SiteWise l'API IoT sur les séries chronologiques.	Séries SiteWise chronologiques sur l'IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Activité de TwinMaker l'API IoT sur une entité.	TwinMaker Entité IoT	`AWS::IoTTwinMaker::Entity`
	Activité de TwinMaker l'API IoT sur un espace de travail.	Espace de TwinMaker travail IoT	`AWS::IoTTwinMaker::Workspace`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Kendra Intelligent Ranking (Classement intelligent Amazon Kendra)	Activité de l'API de classement intelligent Amazon Kendra sur les plans d'exécution de réévaluation.	Classement Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (pour Apache Cassandra)	Activité de l'API Amazon Keyspaces sur une table.	Table Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	Activité de l'API Kinesis Data Streams sur les flux.	Kinesis Stream	`AWS::Kinesis::Stream`
	Activité de l'API Kinesis Data Streams sur les utilisateurs de streams.	Consommateur de Kinesis Stream	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis	Activité de l'API Kinesis Video Streams sur les flux vidéo, tels que les appels `GetMedia` vers `PutMedia` et.	Flux vidéo Kinesis	`AWS::KinesisVideo::Stream`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Managed Blockchain	Activité de l'API Amazon Managed Blockchain sur un réseau.	Réseau Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Appels Amazon Managed Blockchain JSON-RPC sur les nœuds Ethereum, tels que `eth_getBalance` ou `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Graphe Amazon Neptune	Les activités de l'API de données, par exemple les requêtes, les algorithmes ou la recherche vectoriel le, sur un graphe Neptune.	Graphe Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Connecteur pour l'activité de l'API Active Directory.	AWS Private CA Connecteur pour Active Directory	`AWS::PCAConnectorAD::Connector`
Applications Amazon Q	Activité de l'API de données sur Amazon Q Apps.	Applications Amazon Q	`AWS::QApps:QApp`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Q Business	Activité de l'API Amazon Q Business sur une application.	Application Amazon Q Business	`AWS::QBusiness::Application`
	Activité de l'API Amazon Q Business sur une source de données.	Source de données Amazon Q Business	`AWS::QBusiness::DataSource`
	Activité de l'API Amazon Q Business sur un index.	Indice Amazon Q Business	`AWS::QBusiness::Index`
	Activité de l'API Amazon Q Business dans le cadre d'une expérience Web.	Expérience Web Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Activité de l'API Amazon RDS sur un cluster de base de données.	API de données RDS - Cluster de bases de données	`AWS::RDS::DBCluster`
Amazon S3	Activité de l'API Amazon S3 sur les points d'accès.	Points d'accès S3	`AWS::S3::AccessPoint`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de l'API des points d'accès Amazon S3 Object Lambda, comme les appels vers `CompleteMultipartUpload` et. `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Activité de l'API au niveau de l'objet Amazon S3 on Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Activité d'Amazon sur les terminaux.	SageMaker point final	`AWS::SageMaker::Endpoint`
	Activité de SageMaker l'API Amazon sur les magasins de fonctionnalités.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de SageMaker l'API Amazon sur les composants des essais expérimentaux.	SageMaker composant d'essai expérimental sur les métriques	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Opérations d'API `Publish` d'Amazon SNS sur les points de terminaison de la plateforme.	Point de terminaison de la plateforme SNS	`AWS::SNS::PlatformEndpoint`
	Opérations d'API `Publish` et `PublishBatch` d'Amazon SNS sur des rubriques.	Rubrique SNS	`AWS::SNS::Topic`
Amazon SQS	Activité de l'API Amazon SQS sur les messages.	SQS	`AWS::SQS::Queue`
AWS Step Functions	Activité de l'API Step Functions sur une machine à états.	Machine d'état Step Functions	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain Activité de l'API sur une instance.	Chaîne d'approvisionnement	`AWS::SCN::Instance`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon SWF	Activité de l'API Amazon SWF sur les domaines.	Domaine SWF	`AWS::SWF::Domain`
AWS Systems Manager	Activité de l'API Systems Manager sur les canaux de contrôle.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Activité de l'API Systems Manager sur les nœuds gérés.	Nœud géré par Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Activité de l'API `Query` d'Amazon Timestream sur des bases de données.	Base de données Timestream	`AWS::Timestream::Database`
	Activité de l'API `Query` d'Amazon Timestream sur des tables.	Table Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Activité de l'API Amazon Verified Permissions sur un magasin de politiques.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Activité de l'API Thin Client sur un appareil.	Appareil client léger	`AWS::ThinClient::Device`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	WorkSpaces Activité de l'API Thin Client dans un environnement.	Client léger d'environnement	`AWS::ThinClient::Environment`
AWS X-Ray	Activité de l'API X-Ray sur les traces.	X-Ray Trace	`AWS::XRay::Trace`

Les événements de données ne sont pas journalisés par défaut lorsque vous créez un magasin de données d'événement. Pour enregistrer CloudTrail les événements liés aux données, vous devez ajouter explicitement les ressources prises en charge ou les types de ressources pour lesquels vous souhaitez collecter des activités. Pour plus d'informations, consultez Création d'un journal de suivi et Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console.

Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour les CloudTrail tarifs, voir AWS CloudTrail Tarification.

L'exemple suivant montre un enregistrement de journal unique d'un événement de données pour l'action Amazon SNS. `Publish`


```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
```

```
}
```

L'exemple suivant montre un enregistrement de journal unique d'un événement de données pour l'action Amazon Cognito`GetCredentialsForIdentity`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```

Événements Insights

CloudTrail Les événements Insights capturent le taux d'appels d'API ou les taux d'erreur inhabituels de votre AWS compte en analysant les activités CloudTrail de gestion. Les événements Insights fournissent des informations pertinentes, telles que l'API associée, le code d'erreur, l'heure de l'incident et les statistiques, ce qui vous aide à comprendre et à agir par rapport à l'activité inhabituelle. Contrairement aux autres types d'événements enregistrés dans un CloudTrail magasin de données de suivi ou d'événements, les événements Insights sont enregistrés uniquement lorsque des modifications sont CloudTrail détectées dans l'utilisation de l'API de votre compte ou dans la journalisation du taux d'erreur qui diffèrent considérablement des modèles d'utilisation habituels du compte.

Voici des exemples d'activité susceptibles de générer des événements Insights :

- Votre compte ne consigne généralement pas plus de 20 appels d'API `deleteBucket` Amazon S3 par minute, mais commence à consigner une moyenne de 100 appels d'API `deleteBucket` par minute. Un événement Insights est enregistré au début de l'activité inhabituelle, et un autre événement Insights est enregistré pour marquer la fin de l'activité inhabituelle.
- Votre compte enregistre généralement 20 appels par minute à l'API `AuthorizeSecurityGroupIngress` Amazon EC2, mais commence à ne consigner aucun appel à `AuthorizeSecurityGroupIngress`. Un événement Insights est enregistré au début de l'activité inhabituelle, et dix minutes plus tard, lorsque l'activité inhabituelle se termine, un autre événement Insights est journalisé pour marquer la fin de l'activité inhabituelle.
- En règle générale, votre compte se connecte à moins d'une erreur `AccessDeniedException` sur une période de sept jours sur AWS Identity and Access Management l'API, `DeleteInstanceProfile`. Votre compte commence à journaliser en moyenne 12 erreurs `AccessDeniedException` par minute sur `DeleteInstanceProfile` l'appel API. Un événement Insights est journalisé au début de l'activité de taux d'erreur inhabituelle, et un autre événement Insights est journalisé pour marquer la fin de l'activité inhabituelle.

Ces exemples sont fournis à titre d'illustration seulement. Vos résultats peuvent varier en fonction de votre cas d'utilisation.

Pour enregistrer les événements CloudTrail Insights, vous devez activer explicitement les événements Insights sur un magasin de données de parcours ou d'événements nouveau ou existant. Pour plus d'informations sur la création d'un journal de suivi, consultez Création d'un journal de suivi. Pour plus d'informations concernant la création d'un entrepôt de données d'événement, veuillez consulter Créez un magasin de données d'événements pour les événements CloudTrail Insights à l'aide de la console.

Des frais supplémentaires s'appliquent pour les événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.

Deux événements sont enregistrés pour signaler une activité inhabituelle dans CloudTrail Insights : un événement de début et un événement de fin. L'exemple suivant présente un enregistrement de journal d'un événement Insights qui s'est produit lorsque l'API `CompleteLifecycleAction` de la scalabilité automatique des applications a été appelée un nombre inhabituel de fois. Pour les événements Insights, la valeur de `eventCategory` est `Insight`. Un bloc `insightDetails` identifie l'état, la source, le nom, le type Insights et le contexte de l'événement, ainsi que des statistiques et attributions. Pour plus d'informations sur le bloc `insightDetails`, consultez CloudTrail `insightDetails`Élément Insights.


```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
```

```
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
                    }]
                }]
```

```
            }
        },
        "eventCategory": "Insight"
    }
```

Journalisation des événements de gestion

Par défaut, les journaux de suivi et les entrepôts de données d'événement journalisent les événements de gestion et n'incluent pas les événements de données ou les événements Insights.

Des frais supplémentaires s'appliquent pour les événements de données ou Insights. Pour plus d'informations, consultez AWS CloudTrail Pricing (Tarification CTlong).

Table des matières

Événements de gestion

Les événements de gestion fournissent une visibilité sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom opérations de plan de contrôle. Les événements de gestion sont notamment les suivants:

- Configuration de la sécurité (par exemple, les opérations API `AttachRolePolicy` IAM)

- Enregistrement des appareils (par exemple, les opérations API `CreateDefaultVpc` Amazon EC2)
- Configuration des règles de routage des données (par exemple, les opérations API `CreateSubnet` Amazon EC2)
- Configuration de la journalisation (par exemple, les opérations AWS CloudTrail `CreateTrail` d'API)

Les événements de gestion peuvent aussi inclure les événements non API qui se produisent dans votre compte. Par exemple, lorsqu'un utilisateur se connecte à votre compte, CloudTrail enregistre l'`ConsoleLogin`événement. Pour plus d'informations, consultez Événements non liés à l'API capturés par CloudTrail.

Par défaut, les journaux de suivi et les entrepôts de données d'événement sont configurés pour journaliser les événements de gestion.

> **Note**
>
> La fonctionnalité CloudTrail d'historique des événements ne prend en charge que les événements de gestion. Vous ne pouvez pas exclure AWS KMS les événements de l'API Amazon RDS Data de l'historique des événements ; les paramètres que vous appliquez à un magasin de données de suivi ou d'événement ne s'appliquent pas à l'historique des événements. Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.

Enregistrement des événements de gestion à l'aide du AWS Management Console

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Pour mettre à jour un parcours, ouvrez la page Sentiers de la CloudTrail console et choisissez le nom du parcours.

   Pour mettre à jour un magasin de données d'événements, ouvrez la page Stockages de données d'événements de la CloudTrail console et choisissez le nom du magasin de données d'événements.
3. Pour Management events (Événements de gestion), choisir Edit (Modifier).

- Choisissez si vous voulez que votre journal de suivi journalise les événements Lecture, les événements Écriture, ou les deux.
- Choisissez Exclure les AWS KMS événements pour filtrer AWS Key Management Service (AWS KMS) les événements de votre historique ou de votre banque de données d'événements. Le paramètre par défaut est d'inclure tous les AWS KMS événements.

  L'option permettant de consigner ou d'exclure AWS KMS des événements n'est disponible que si vous enregistrez les événements de gestion sur votre parcours ou dans votre banque de données d'événements. Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

  AWS KMS des actions telles que `EncryptDecrypt`, et génèrent `GenerateDataKey` généralement un grand volume (plus de 99 %) d'événements. Ces actions sont désormais journalisées en tant qu'événements Lecture. Les AWS KMS actions pertinentes à faible volume telles que `DisableDelete`, et `ScheduleKey` (qui représentent généralement moins de 0,5 % du volume d' AWS KMS événements) sont enregistrées en tant qu'événements d'écriture.

  Pour exclure des événements importants tels que`Encrypt`, et `DecryptGenerateDataKey`, tout en enregistrant les événements pertinents tels que`Disable`, `Delete` et`ScheduleKey`, choisissez de consigner les événements de gestion d'écriture et décochez la case Exclure les AWS KMS événements.
- Choisissez Exclure les événements API de données Amazon RDS pour filtrer les événements d'API de données du service Amazon Relational Database hors de votre journal de suivi ou de votre entrepôt de données d'événement. Le paramètre par défaut consiste à inclure tous les événements d'API de données Amazon RDS. Pour plus d'informations sur les événements d'API Amazon RDS Data API, consultez Journalisation des appels d'API de données avec AWS CloudTrail dans le Guide de l'utilisateur Amazon RDS pour Aurora.

4. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Evénements de lecture et d'écriture

Quand vous configurez votre journal de suivi ou votre entrepôt de données d'événement pour journaliser les événements de gestion, vous pouvez spécifier si voulez les événements en lecture seule, les événements en écriture seule ou les deux.

- Read (Lire)

  Les événements en lecture seule englobent les opérations API qui lisent vos ressources, mais n'y apportent pas de modifications. Par exemple, les événements en lecture seule comprennent les opérations API `DescribeSecurityGroups` et `DescribeSubnets` de Amazon EC2. Ces opérations renvoient uniquement les informations relatives à vos ressources Amazon EC2 et elles ne modifient pas vos configurations.

- Write (Écrire)

  Les événements en écriture seule englobent les opérations d'API qui modifient (ou peuvent modifier) vos ressources. Par exemple, les opérations API `RunInstances` et `TerminateInstances` de Amazon EC2 modifient vos instances.

Exemple : la journalisation des événements lire et écrire pour des journaux de suivi distincts

L'exemple suivant montre comment configurer vos journaux de suivi pour fractionner l'activité de journalisation d'un compte dans des compartiments S3 distincts: un compartiment reçoit les événements en lecture seule, et le second, les événements en écriture seule.

1. Vous créez un journal de suivi et choisissez un compartiment S3 nommé `read-only-bucket` pour recevoir les fichiers journaux. Ensuite, vous mettez à jour le journal de suivi pour spécifier que vous voulez les événements de gestion Read (Lire).
2. Vous créez un deuxième journal de suivi et choisissez un compartiment S3 nommé `write-only-bucket` pour recevoir les fichiers journaux. Ensuite, vous mettez à jour le journal de suivi pour spécifier que vous voulez les événements de gestion Write (Écrire).
3. Les opérations API `DescribeInstances` et `TerminateInstances` Amazon EC2 sont effectuées dans votre compte.
4. L'opération API `DescribeInstances` est un événement en lecture seule et elle correspond aux paramètres du premier journal de suivi. L'événement est journalisé et transmis au `read-only-bucket` par le journal de suivi.
5. L'opération API `TerminateInstances` est un événement en écriture seule et elle correspond aux paramètres du deuxième journal de suivi. L'événement est journalisé et livré au par le journal de suivi `write-only-bucket`.

Consignation des événements avec le AWS Command Line Interface

Vous pouvez configurer vos journaux de suivi ou vos entrepôts de données d'événement de manière à ce qu'ils journalisent les événements de gestion et de données à l'aide de AWS CLI.

Rubriques

Exemples : journalisation des événements de gestion pour les journaux de suivi

Pour voir si votre journal de suivi journalise les événements de gestion, exécutez la `get-event-selectors` commande.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

L'exemple suivant renvoie les paramètres par défaut pour un journal de suivi. Par défaut, les journaux de suivi journalisent tous les événements de gestion, les événements du journal provenant de toutes les sources d'événement, mais ne consignent pas les événements de données.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

Vous pouvez utiliser des sélecteurs d'événements de base ou avancés pour consigner les événements de gestion. Vous ne pouvez pas appliquer à la fois les sélecteurs d'événements et

les sélecteurs d'événements avancés à une piste. Si vous appliquez des sélecteurs d'événements avancés à un journal de suivi, tous les sélecteurs d'événements de base existants sont remplacés. Les sections suivantes fournissent des exemples de journalisation des événements de gestion à l'aide de sélecteurs d'événements avancés et de sélecteurs d'événements de base.

Rubriques

Exemples : enregistrement des événements de gestion pour les sentiers à l'aide de sélecteurs d'événements avancés

L'exemple suivant crée un sélecteur d'événements avancé pour un journal nommé *TrailName* pour inclure les événements de gestion en lecture seule et en écriture seule (en omettant le `readOnly` sélecteur), mais pour exclure () les événements. AWS Key Management Service AWS KMSÉtant donné que les AWS KMS événements sont traités comme des événements de gestion et qu'ils peuvent être nombreux, ils peuvent avoir un impact important sur votre CloudTrail facture si vous disposez de plusieurs pistes qui enregistrent les événements de gestion.

Si vous choisissez de ne pas consigner les événements de gestion, AWS KMS ceux-ci ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des AWS KMS événements.

Pour recommencer à enregistrer AWS KMS des événements dans un journal, supprimez le `eventSource` sélecteur et réexécutez la commande.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

L'exemple renvoie le sélecteur d'événements avancés configuré pour le journal de suivi.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour redémarrer la journalisation des événements exclus dans un journal de suivi, supprimez le sélecteur `eventSource`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

L'exemple suivant crée un sélecteur d'événements avancé pour un journal nommé de manière *TrailName*à inclure les événements de gestion en lecture seule et en écriture seule (en omettant le `readOnly` sélecteur), mais pour exclure les événements de gestion de l'API Amazon RDS Data. Pour exclure les événements de gestion de l'API Amazon RDS Data, spécifiez la source de l'événement Amazon RDS Data API dans la valeur de chaîne du `eventSource` champ :. `rdsdata.amazonaws.com`

Si vous choisissez de ne pas enregistrer les événements de gestion, les événements de gestion de l'API Amazon RDS Data ne sont pas enregistrés et vous ne pouvez pas modifier les paramètres de journalisation des événements de l'API Amazon RDS Data.

Pour recommencer à consigner les événements de gestion de l'API Amazon RDS Data dans un journal, supprimez le `eventSource` sélecteur et réexécutez la commande.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

L'exemple renvoie le sélecteur d'événements avancés configuré pour le journal de suivi.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Pour redémarrer la journalisation des événements exclus dans un journal de suivi, supprimez le sélecteur `eventSource`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Exemples : enregistrement des événements de gestion pour les sentiers à l'aide de sélecteurs d'événements de base

Pour configurer votre journal de suivi de sorte qu'il journalise les événements de gestion, exécutez la `put-event-selectors` commande. L'exemple suivant montre comment configurer votre journal de suivi pour inclure tous les événements de gestion pour deux objets S3. Vous pouvez spécifier de 1 à 5 sélecteurs d'événements pour un journal d'activité. Vous pouvez spécifier de 1 à 250 ressources de données pour un journal d'activité.

> **Note**
>
> Le nombre maximal de ressources de données S3 est 250, quel que soit le nombre de sélecteurs d'événements.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

L'exemple suivant renvoie le sélecteur d'événements configuré pour le journal de suivi.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
```

```
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

Pour exclure des événements AWS Key Management Service (AWS KMS) des journaux d'un suivi, exécutez la `put-event-selectors` commande et ajoutez l'attribut `ExcludeManagementEventSources` avec une valeur de`kms.amazonaws.com`. L'exemple suivant crée un sélecteur d'événements pour un journal dont le nom inclut les événements *`TrailName`*de gestion en lecture seule et en écriture seule, mais exclut les événements. AWS KMS Étant donné que cela AWS KMS peut générer un volume élevé d'événements, l'utilisateur de cet exemple peut souhaiter limiter les événements afin de gérer le coût d'un parcours.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

L'exemple renvoie le sélecteur d'événements configuré pour le journal de suivi.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

Pour exclure les événements de gestion de l'API Amazon RDS Data des journaux d'un suivi, exécutez la `put-event-selectors` commande et ajoutez l'attribut `ExcludeManagementEventSources` avec une valeur de`rdsdata.amazonaws.com`. L'exemple suivant crée un sélecteur d'événements pour un parcours nommé de manière *`TrailName`*à inclure les événements de gestion en lecture seule et en écriture seule, mais à exclure les événements de gestion de l'API Amazon RDS Data. Étant donné que l'API Amazon RDS Data peut générer un volume élevé d'événements de gestion, l'utilisateur de cet exemple peut souhaiter limiter les événements afin de gérer le coût d'un suivi.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
}
```

Pour recommencer à AWS KMS consigner les événements ou à gérer l'API Amazon RDS Data dans un journal, transmettez une chaîne vide comme valeur de`ExcludeManagementEventSources`, comme indiqué dans la commande suivante.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Pour enregistrer les AWS KMS événements pertinents dans un journal, tels que`Disable`, `Delete` et`ScheduleKey`, mais exclure les AWS KMS événements à volume élevé tels que`Encrypt`, et `DecryptGenerateDataKey`, consigner les événements de gestion en écriture uniquement, et conserver le paramètre par défaut de journalisation AWS KMS des événements, comme indiqué dans l'exemple suivant.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Exemples : journalisation des événements de gestion pour les entrepôts de données d'événement

Pour voir si votre entrepôt de données d'événement inclut les événements de gestion, exécutez la commande get-event-data-store.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Voici un exemple de réponse. Les heures de création et de dernière mise à jour sont au format `timestamp`.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
```

```
}
```

Pour créer un entrepôt de données d'événement qui inclut tous les événements de gestion, vous devez exécuter la commande create-event-data-store. Il n'est pas nécessaire de spécifier des sélecteurs d'événements avancés pour inclure tous les événements de gestion.

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

Pour créer un magasin de données d'événements qui exclut AWS Key Management Service (AWS KMS) les événements, exécutez la `create-event-data-store` commande et `eventSource` spécifiez une valeur différente`kms.amazonaws.com`. L'exemple suivant crée un magasin de

données d'événements qui inclut des événements de gestion en lecture seule et en écriture seule, mais exclut les événements. AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
```

```
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Pour créer un magasin de données d'événements qui exclut les événements de gestion de l'API Amazon RDS Data, exécutez la `create-event-data-store` commande et spécifiez une valeur `rdsdata.amazonaws.com` différente. `eventSource` L'exemple suivant crée un entrepôt de données d'événement qui inclut les événements de gestion en lecture seule et en écriture seule, en excluant les événements API de données Amazon RDS.

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
```

```
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Journalisation des événements avec les AWS SDK

Utilisez cette GetEventSelectorsopération pour voir si votre sentier enregistre les événements de gestion relatifs à un sentier. Vous pouvez configurer vos sentiers pour enregistrer les événements de gestion associés à l'PutEventSelectorsopération. Pour plus d'informations, consultez la page Référence de l'API AWS CloudTrail.

Exécutez l'GetEventDataStoreopération pour voir si votre banque de données d'événements inclut des événements de gestion. Vous pouvez configurer vos magasins de données d'événements pour inclure les événements de gestion en exécutant les UpdateEventDataStoreopérations CreateEventDataStoreor. Pour plus d'informations, consultez les pages Créez, mettez à jour et gérez des banques de données d'événements à l'aide du AWS CLI et Référence de l'API AWS CloudTrail.

Envoi d'événements à Amazon CloudWatch Logs

Pour les sentiers, CloudTrail prend en charge l'envoi de données et d'événements de gestion à CloudWatch Logs. Lorsque vous configurez votre journal pour envoyer des événements à votre groupe de CloudWatch journaux Logs, il CloudTrail envoie uniquement les événements que vous spécifiez dans votre journal. Par exemple, si vous configurez votre journal pour qu'il enregistre uniquement les événements de gestion, il transmet les événements de gestion uniquement à votre groupe de CloudWatch journaux journaux. Pour plus d'informations, voir Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.

Journalisation des événements de données

Cette section décrit comment enregistrer des événements de données à l'aide de la CloudTrail console et AWS CLI.

Par défaut, les journaux de suivi et les entrepôts de données d'événement ne journalisent pas les événements de données. Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.

Les événements de données fournissent une visibilité sur les opérations de ressource exécutées sur ou dans une ressource. Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé.

Les événements de données incluent notamment :

- Activité de l'API au niveau des objets Amazon S3 (par exemple, `GetObject`, `DeleteObject`, et opérations d'`PutObject`API) sur des objets dans des compartiments S3.
- AWS Lambda activité d'exécution de fonctions (l'`Invoke`API).
- CloudTrail `PutAuditEvents`activité sur un chenal CloudTrail lacustre utilisé pour enregistrer des événements provenant de l'extérieur AWS.
- Opérations d'API `Publish` et `PublishBatch` d'Amazon SNS sur des rubriques.

Vous pouvez utiliser des sélecteurs d'événements avancés pour créer des sélecteurs précis, qui vous aident à contrôler les coûts en enregistrant uniquement les événements spécifiques présentant un intérêt pour vos cas d'utilisation. Par exemple, vous pouvez utiliser des sélecteurs d'événements avancés pour enregistrer des appels d'API spécifiques en ajoutant un filtre sur le `eventName` champ. Pour plus d'informations, consultez Filtrer les événements liés aux données à l'aide de sélecteurs d'événements avancés.

> **Note**
>
> Les événements enregistrés par vos parcours sont disponibles sur Amazon EventBridge. Par exemple, si vous choisissez de journaliser les événements de données pour les objets S3, mais pas les événements de gestion, votre journal de suivi ne traite et ne journalise que les événements de données pour les objets S3 spécifiés. Les événements de données pour ces objets S3 sont disponibles sur Amazon EventBridge. Pour plus d'informations, consultez

la section Événements liés AWS aux services dans le guide de EventBridge l'utilisateur Amazon.

Table des matières

    - Filtrer les événements de données par readOnly valeur à l'aide du AWS Management Console
    - Filtrer les événements de données par readOnly valeur à l'aide du AWS CLI
- La journalisation des événements de données pour la conformité AWS Config
- Enregistrement des événements liés aux données avec les AWS SDK
- Envoi d'événements à Amazon CloudWatch Logs

Événements de données

Le tableau suivant indique les types d'événements de données disponibles pour les journaux de suivi et les entrepôts de données d'événement. La colonne Type d'événement de données (console) indique la sélection appropriée dans la console. La colonne de valeur resources.type indique la `resources.type` valeur que vous devez spécifier pour inclure les événements de données de ce type dans votre magasin de données de suivi ou d'événement à l' AWS CLI aide des API or. CloudTrail

Pour les traces, vous pouvez utiliser des sélecteurs d'événements de base ou avancés pour enregistrer les événements de données relatifs aux objets Amazon S3, aux fonctions Lambda et aux tables DynamoDB (illustrés dans les trois premières lignes du tableau). Vous ne pouvez utiliser que des sélecteurs d'événements avancés pour enregistrer les types d'événements de données indiqués dans les lignes restantes.

Pour les entrepôts de données d'événement, vous ne pouvez utiliser que des sélecteurs d'événements avancés pour inclure les événements de données.

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon DynamoDB	Activité de l'API au niveau des éléments Amazon DynamoDB sur les tables (par exemplePutItem,Dele	DynamoDB	`AWS::DynamoDB::Table`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	m , et les opérations d'API). UpdateItem **Note** Pour les tables ayant les flux activés, le champ resources dans l'événement de données contient à la fois AWS::DynamoDB::Stream et AWS::DynamoDB::Table . Si vous spécifiez AWS::DynamoDB::Table comme resources.type , les événements de table DynamoDB et les		

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	événement s de flux DynamoDB sont journalis és par défaut. Pour exclure les [événement s de flux], ajoutez un filtre sur le `eventName` champ.		
AWS Lambda	AWS Lambda activité d'exécuti on de fonctions (l'`Invoke`API).	Lambda	`AWS::Lambda::Function`
Amazon S3	[Activité de l'API au niveau des objets Amazon S3] (par exemple, `GetObject` `DeleteObj ect` , et opérations d'`PutObject` API) sur des objets dans des compartiments S3.	S3	`AWS::S3::Object`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS AppConfig	AWS AppConfig Activité de l'API pour les opérations de configuration telles que les appels vers `StartConfigurationSession` et `GetLatestConfiguration`.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Échange de données B2B	Activité de l'API d'échange de données B2B pour les opérations du transformateur telles que les appels vers `GetTransformerJob` et `StartTransformerJob`.	Échange de données B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Activité de l'API Amazon Bedrock sur un alias d'agent.	Alias d'agent Bedrock	`AWS::Bedrock::AgentAlias`
	Activité de l'API Amazon Bedrock sur une base de connaissances.	Base de connaissances Bedrock	`AWS::Bedrock::KnowledgeBase`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon CloudFront	CloudFront Activité de l'API sur un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Activité de l'API sur un espace de noms.	AWS Cloud Map espace de nom	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Activité de l'API sur un service.	AWS Cloud Map web	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` activité sur un chenal CloudTrail lacustre utilisé pour enregistrer des événements provenant de l'extérieur AWS.	CloudTrail canal	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Activité de CodeWhisperer l'API Amazon lors d'une personnalisation.	CodeWhisperer personnalisation	`AWS::CodeWhisperer::Customization`
	Activité de CodeWhisperer l'API Amazon sur un profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Cognito	Activité de l'API Amazon Cognito sur les réserves d'identités Amazon Cognito.	Réserves d'identités Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Activité de l'API Amazon DynamoDB sur les flux.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	API directes Amazon Elastic Block Store (EBS) telles que `PutSnapshotBlock`, `GetSnapshotBlock`, et `ListChangedBlocks` sur des instantanés Amazon EBS.	API directes Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Activité de l'API Amazon EMR sur un espace de travail de journalisation à écriture anticipée.	Espace de travail de journalisation à écriture anticipée EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Activité de l'API Amazon FinSpace sur les environnements.	FinSpace	`AWS::FinSpace::Environment`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
AWS Glue	AWS Glue Activité de l'API sur les tables créées par Lake Formation. **Note** AWS Glue les événements de données pour les tables ne sont actuellement pris en charge que dans les régions suivantes : • USA Est (Virginie du Nord) • USA Est (Ohio) • USA Ouest (Oregon) • Europe (Irlande) • Région Asie-	Lake Formation	`AWS::Glue::Table`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Pacifique (Tokyo)		
Amazon GuardDuty	Activité de GuardDuty l'API Amazon pour un détecteur.	GuardDuty détecteur	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Activité de l'API sur les magasins de données.	Magasin de données d'imagerie médicale	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Activité de l'API sur les certificats.	Certificat IoT	`AWS::IoT::Certificate`
	AWS IoT Activité de l'API sur les objets.	Un truc lié à l'IoT	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	Activité de l'API Greengrass depuis un appareil principal de Greengrass sur une version de composant . **Note** Greengrass n'enregistre pas les cas de refus d'accès.	Version du composant IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de l'API Greengrass depuis un appareil principal de Greengrass lors d'un déploiement. **Note** Greengrass n'enregistre pas les cas de refus d'accès.	Déploiement de Greengrass pour l'IoT	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Activité de SiteWise l'API IoT sur les actifs.	SiteWise Actif IoT	`AWS::IoTSiteWise::Asset`
	Activité de SiteWise l'API IoT sur les séries chronologiques.	Séries SiteWise chronologiques sur l'IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Activité de TwinMaker l'API IoT sur une entité.	TwinMaker Entité IoT	`AWS::IoTTwinMaker::Entity`
	Activité de TwinMaker l'API IoT sur un espace de travail.	Espace de TwinMaker travail IoT	`AWS::IoTTwinMaker::Workspace`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Kendra Intelligent Ranking (Classement intelligent Amazon Kendra)	Activité de l'API de classement intelligent Amazon Kendra sur les plans d'exécution de réévaluation.	Classement Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (pour Apache Cassandra)	Activité de l'API Amazon Keyspaces sur une table.	Table Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	Activité de l'API Kinesis Data Streams sur les flux.	Kinesis Stream	`AWS::Kinesis::Stream`
	Activité de l'API Kinesis Data Streams sur les consommateurs de flux.	Consommateur de Kinesis Stream	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis	Activité de l'API Kinesis Video Streams sur les flux vidéo, tels que les appels `GetMedia` vers `PutMedia` et.	Flux vidéo Kinesis	`AWS::KinesisVideo::Stream`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Managed Blockchain	Activité de l'API Amazon Managed Blockchain sur un réseau.	Réseau Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Appels Amazon Managed Blockchain JSON-RPC sur les nœuds Ethereum, tels que `eth_getBalance` ou `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Graphe Amazon Neptune	Les activités de l'API de données, par exemple les requêtes, les algorithmes ou la recherche vectoriel le, sur un graphe Neptune.	Graphe Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Connecteur pour l'activité de l'API Active Directory.	AWS Private CA Connecteur pour Active Directory	`AWS::PCAConnectorAD::Connector`
Applications Amazon Q	Activité de l'API de données sur Amazon Q Apps.	Applications Amazon Q	`AWS::QApps:QApp`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon Q Business	Activité de l'API Amazon Q Business sur une application.	Application Amazon Q Business	`AWS::QBusiness::Application`
	Activité de l'API Amazon Q Business sur une source de données.	Source de données Amazon Q Business	`AWS::QBusiness::DataSource`
	Activité de l'API Amazon Q Business sur un index.	Indice Amazon Q Business	`AWS::QBusiness::Index`
	Activité de l'API Amazon Q Business dans le cadre d'une expérience Web.	Expérience Web Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Activité de l'API Amazon RDS sur un cluster de base de données.	API de données RDS - Cluster de bases de données	`AWS::RDS::DBCluster`
Amazon S3	Activité de l'API Amazon S3 sur les points d'accès.	Points d'accès S3	`AWS::S3::AccessPoint`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de l'API des points d'accès Amazon S3 Object Lambda, comme les appels vers `CompleteMultipartUpload` et. `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Activité de l'API au niveau de l'objet Amazon S3 on Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Activité d'Amazon sur les terminaux.	SageMaker point final	`AWS::SageMaker::Endpoint`
	Activité de SageMaker l'API Amazon sur les magasins de fonctionnalités.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	Activité de SageMaker l'API Amazon sur les composants des essais expérimentaux.	SageMaker composant d'essai expérimental sur les métriques	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Opérations d'API `Publish` d'Amazon SNS sur les points de terminaison de la plateforme.	Point de terminaison de la plateforme SNS	`AWS::SNS::PlatformEndpoint`
	Opérations d'API `Publish` et `PublishBatch` d'Amazon SNS sur des rubriques.	Rubrique SNS	`AWS::SNS::Topic`
Amazon SQS	Activité de l'API Amazon SQS sur les messages.	SQS	`AWS::SQS::Queue`
AWS Step Functions	Activité de l'API Step Functions sur une machine à états.	Machine d'état Step Functions	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain Activité de l'API sur une instance.	Chaîne d'approvisionnement	`AWS::SCN::Instance`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
Amazon SWF	Activité de l'API Amazon SWF sur les domaines.	Domaine SWF	`AWS::SWF::Domain`
AWS Systems Manager	Activité de l'API Systems Manager sur les canaux de contrôle.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Activité de l'API Systems Manager sur les nœuds gérés.	Nœud géré par Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Activité de l'API `Query` d'Amazon Timestream sur des bases de données.	Base de données Timestream	`AWS::Timestream::Database`
	Activité de l'API `Query` d'Amazon Timestream sur des tables.	Table Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Activité de l'API Amazon Verified Permissions sur un magasin de politiques.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Activité de l'API Thin Client sur un appareil.	Appareil client léger	`AWS::ThinClient::Device`

Service AWS	Description	Type d'événement de données (console)	valeur resources.type
	WorkSpaces Activité de l'API Thin Client dans un environnement.	Client léger d'environnement	`AWS::ThinClient::Environment`
AWS X-Ray	Activité de l'API X-Ray sur les traces.	X-Ray Trace	`AWS::XRay::Trace`

Pour enregistrer CloudTrail les événements liés aux données, vous devez ajouter explicitement chaque type de ressource pour lequel vous souhaitez collecter l'activité. Pour plus d'informations, consultez Création d'un journal de suivi et Création d'un magasin de données d'CloudTrailévénements pour les événements à l'aide de la console.

Sur un journal de suivi ou un entrepôt de données d'événement à région unique, vous pouvez journaliser les événements de données uniquement pour les ressources auxquelles vous pouvez accéder dans cette région. Bien que les compartiments S3 soient globaux, les AWS Lambda fonctions et les tables DynamoDB sont régionales.

Des frais supplémentaires s'appliquent pour la journalisation des événements de données. Pour les CloudTrail tarifs, consultez la section AWS CloudTrail Tarification.

Exemples : journalisation des événements de données pour les objets Amazon S3

Journalisation des événements de données pour les objets S3 d'un compartiment S3

L'exemple suivant montre comment la journalisation fonctionne lorsque vous configurez la journalisation de tous les événements de données d'un compartiment S3 nommé *`bucket-1`*. Dans cet exemple, l' CloudTrail utilisateur a spécifié un préfixe vide et l'option permettant de consigner les événements de données en lecture et en écriture.

1. Un utilisateur charge un objet sur `bucket-1`.
2. L'opération API `PutObject` est une API au niveau objet Amazon S3. Il est enregistré en tant qu'événement de données dans CloudTrail. Étant donné que l' CloudTrail utilisateur a spécifié un

compartiment S3 avec un préfixe vide, les événements qui se produisent sur n'importe quel objet de ce compartiment sont enregistrés. L'entrepôt de données d'événement ou le journal de suivi traite et journalise l'événement.

3. Un autre utilisateur charge un objet sur `bucket-2`.
4. L'opération API `PutObject` s'est produite sur un objet d'un compartiment S3 qui n'était pas spécifié dans le journal de suivi. L'événement n'est pas journalisé par le journal de suivi ou l'entrepôt de données d'événement.

Journalisation des événements de données pour des objets S3 spécifiques

L'exemple suivant montre comment la journalisation fonctionne lorsque vous configurez un journal de suivi ou un entrepôt de données d'événement pour journaliser les événements d'objets S3 spécifiques. Dans cet exemple, l' CloudTrail utilisateur a spécifié un compartiment S3 nommé ***`bucket-3`***, avec le préfixe ***`my-images`***, et l'option permettant de ne consigner que les événements d'écriture de données.

1. Un utilisateur supprime un objet qui commence par le préfixe `my-images` dans le compartiment, tel que `arn:aws:s3:::bucket-3/my-images/example.jpg`.
2. L'opération API `DeleteObject` est une API au niveau objet Amazon S3. Il est enregistré en tant qu'événement Write data in CloudTrail. L'événement s'est produit sur un objet qui correspond au préfixe et au compartiment S3 spécifiés dans le journal de suivi ou l'entrepôt de données d'événement. L'entrepôt de données d'événement ou le journal de suivi traite et journalise l'événement.
3. Un autre utilisateur supprime un objet avec un préfixe différent dans le compartiment S3, tel que `arn:aws:s3:::bucket-3/my-videos/example.avi`.
4. L'événement s'est produit sur un objet qui ne correspond pas au préfixe spécifié dans votre journal de suivi ou l'entrepôt de données d'événement. L'événement n'est pas journalisé par le journal de suivi ou l'entrepôt de données d'événement.
5. Un utilisateur appelle l'opération API `GetObject` pour l'objet `arn:aws:s3:::bucket-3/my-images/example.jpg`.
6. L'événement est survenu sur un compartiment et un préfixe spécifiés dans le journal de suivi ou l'entrepôt de données d'événement, mais `GetObject` est une API de niveau objet Amazon S3 de type lecture. Il est enregistré en tant qu'événement de lecture de données dans CloudTrail, et le magasin de données de suivi ou d'événement n'est pas configuré pour enregistrer les

événements de lecture. L'événement n'est pas journalisé par le journal de suivi ou l'entrepôt de données d'événement.

> **Note**
>
> Si vous journalisez des événements de données pour des compartiments Amazon S3 spécifiques, nous vous déconseillons l'utilisation d'un compartiment Amazon S3 pour lequel vous journalisez des événements de données pour recevoir des fichiers journaux que vous avez spécifiés dans la section des événements de données. L'utilisation du même compartiment S3 permet à votre journal de suivi de consigner un événement de données chaque fois que les fichiers journaux sont transmis à votre compartiment Amazon S3. Les fichiers journaux sont composés d'un groupe d'événements transmis à certains intervalles, ce n'est donc pas un rapport 1:1 événement-fichier journal. L'événement est journalisé dans le fichier journal suivant. Par exemple, lors de la CloudTrail livraison de journaux, l'`PutObject`événement se produit dans le compartiment S3. Si le compartiment S3 est également spécifié dans la section des événements de données, l'événement `PutObject` est traité et journalisé par le journal d'activité en tant qu'événement de données. Cette action est un autre événement `PutObject`, qui est traité et enregistré à nouveau par le journal d'activité.
>
> Pour éviter de consigner les événements de données pour le compartiment Amazon S3 dans lequel vous recevez les fichiers journaux si vous configurez un suivi pour consigner tous les événements de données Amazon S3 dans votre AWS compte, envisagez de configurer la livraison des fichiers journaux vers un compartiment Amazon S3 appartenant à un autre AWS compte. Pour plus d'informations, consultez Réception de fichiers CloudTrail journaux provenant de plusieurs comptes.

Journalisation des événements de données pour les objets S3 dans d'autres AWS comptes

Lorsque vous configurez votre journal pour consigner les événements liés aux données, vous pouvez également spécifier des objets S3 appartenant à d'autres AWS comptes. Lorsqu'un événement se produit sur un objet spécifié, CloudTrail évalue si l'événement correspond aux traces de chaque compte. Si l'événement correspond aux paramètres d'un journal d'activité, il est traité et journalisé par le journal de suivi pour ce compte. Généralement, les appelants d'API et les propriétaires de ressources peuvent recevoir des événements.

Si vous êtes propriétaire d'un objet S3 et que vous le précisez dans votre journal d’activité, les événements du journal qui se produisent sur l'objet dans votre compte sont journalisés par le journal de suivi. Étant donné que vous êtes propriétaire de l’objet, votre journal d’activité enregistre également les événements du journal lorsque d’autres comptes appellent l’objet.

Si vous spécifiez un objet S3 dans votre journal d’activité, et qu'un autre compte est propriétaire de l'objet, seuls les événements du journal qui se produisent sur cet objet dans votre compte sont enregistrés par votre suivi. Les événements du journal qui se produisent dans d'autres comptes ne sont pas enregistrés par votre journal d’activité.

Exemple : journalisation des événements de données d'un objet Amazon S3 pour deux comptes AWS

L'exemple suivant montre comment deux AWS comptes sont configurés CloudTrail pour consigner des événements pour le même objet S3.

1. Dans votre compte, vous souhaitez que votre journal de suivi journalise les événements de données pour tous les objets de votre compartiment S3 nommés `owner-bucket`. Vous configurez le journal de suivi en spécifiant le compartiment S3 avec un préfixe d'objet vide.
2. Bob a un compte distinct qui dispose d’un accès au compartiment S3. Il souhaite également journaliser les événements de données pour tous les objets dans le même compartiment S3. Pour son journal de suivi, il configure le journal de suivi et spécifie le même compartiment S3 avec un préfixe d'objet vide.
3. Bob charge un objet dans le compartiment S3 avec l’opération d’API `PutObject`.
4. Cet événement s'est produit dans son compte et il correspond aux paramètres pour son journal de suivi. L'événement est traité et journalisé par le journal de suivi de Bob.
5. Puisque vous êtes propriétaire du compartiment S3 et que l'événement correspond aux paramètres pour votre journal de suivi, ce même événement est également traité et journalisé par votre journal de suivi. Comme il existe désormais deux copies de l'événement (l'une connectée à la trace de Bob et l'autre connectée à la vôtre), CloudTrail deux copies de l'événement de données sont facturées.
6. Vous chargez un objet dans le compartiment S3.
7. Cet événement se produit dans votre compte et il correspond aux paramètres pour votre journal de suivi. L'événement est traité et journalisé par votre journal de suivi.
8. Comme l'événement ne s'est pas produit dans le compte de Bob et qu'il ne possède pas le compartiment S3, le suivi de Bob n'enregistre pas l'événement. CloudTrail des frais pour une seule copie de cet événement de données.

Exemple : enregistrement des événements de données pour tous les compartiments, y compris un compartiment S3 utilisé par deux comptes AWS

L'exemple suivant montre le comportement de journalisation lorsque l'option Sélectionner tous les compartiments S3 de votre compte est activée pour les traces qui collectent des événements de données dans un AWS compte.

1. Dans votre compte, vous souhaitez que votre journal de suivi journalise les événements de données pour tous les compartiments S3. Vous configurez le journal de suivi en choisissant les événements Lecture, les événements Écriture ou les deux pour Tous les compartiments S3 actuels et futurs dans Événements de données.
2. Bob dispose d'un compte distinct qui a été autorisé à accéder à un compartiment S3 dans votre compte. Il veut journaliser les événements de données pour le compartiment auquel il a accès. Il configure son journal de suivi de manière à obtenir des événements de données pour tous les compartiments S3.
3. Bob charge un objet dans le compartiment S3 avec l'opération d'API `PutObject`.
4. Cet événement s'est produit dans son compte et il correspond aux paramètres pour son journal de suivi. L'événement est traité et journalisé par le journal de suivi de Bob.
5. Puisque vous êtes propriétaire du compartiment S3 et que l'événement correspond aux paramètres pour votre journal de suivi, ce même événement est également traité et journalisé votre journal de suivi. Comme il existe désormais deux copies de l'événement (l'une connectée à la trace de Bob et l'autre connectée à la vôtre), une copie de l'événement de données est CloudTrail facturée à chaque compte.
6. Vous chargez un objet dans le compartiment S3.
7. Cet événement se produit dans votre compte et il correspond aux paramètres pour votre journal de suivi. L'événement est traité et journalisé par votre journal de suivi.
8. Comme l'événement ne s'est pas produit dans le compte de Bob et qu'il ne possède pas le compartiment S3, le suivi de Bob n'enregistre pas l'événement. CloudTrail des frais pour une seule copie de cet événement lié aux données enregistrée sur votre compte.
9. Un troisième utilisateur, Mary, a accès au compartiment S3 et exécute une opération `GetObject` sur le compartiment. Elle dispose d'un journal de suivi configuré de manière à journaliser les événements de données sur tous les compartiments S3 de son compte. Parce qu'elle appelle l'API, elle CloudTrail enregistre un événement de données dans son historique. Bien que Bob ait accès au compartiment, il n'est pas le propriétaire de la ressource, donc aucun événement n'est journalisé dans son journal de suivi cette fois. En tant que propriétaire de la

ressource, vous recevez un événement sur votre parcours concernant l'`GetObject`opération que Mary a appelée. CloudTraildébite votre compte et celui de Mary pour chaque copie de l'événement lié aux données : une copie sur les traces de Mary et une sur la vôtre.

Événements en lecture seule et en écriture seule

Quand vous configurez votre journal de suivi ou votre entrepôt de données d'événement pour journaliser les événements de données et de gestion, vous pouvez spécifier si voulez les événements en lecture seule, les événements en écriture seule ou les deux.

- Lecture

  Les événements Lire englobent les opérations d'API qui lisent vos ressources, mais n'y apportent aucune modification. Par exemple, les événements en lecture seule comprennent les opérations d'API `DescribeSecurityGroups` et `DescribeSubnets` Amazon EC2. Ces opérations renvoient uniquement les informations relatives à vos ressources Amazon EC2 et elles ne modifient pas vos configurations.
- Write (Écrire)

  Les événements Écrire englobent les opérations d'API qui modifient (ou sont susceptibles de modifier) vos ressources. Par exemple, les opérations API `RunInstances` et `TerminateInstances` Amazon EC2 modifient vos instances.

Exemple : la journalisation des événements lire et écrire pour des journaux de suivi distincts

L'exemple suivant montre comment configurer vos journaux de suivi pour fractionner l'activité de journalisation d'un compte dans des compartiments S3 distincts: un compartiment reçoit les événements en lecture seule, et le second, les événements en écriture seule.

1. Vous créez un journal de suivi et choisissez un compartiment S3 nommé `read-only-bucket` pour recevoir les fichiers journaux. Ensuite, vous mettez à jour le journal de suivi pour spécifier que vous voulez les événements de gestion et de données Read Lire().
2. Vous créez un deuxième journal de suivi et choisissez un compartiment S3 nommé `write-only-bucket` pour recevoir les fichiers journaux. Ensuite, vous mettez à jour le journal de suivi pour spécifier que vous voulez les événements de gestion et de données Write (Ecrire).
3. Les opérations API `DescribeInstances` et `TerminateInstances` Amazon EC2 sont effectuées dans votre compte.

4. L'opération API `DescribeInstances` est un événement en lecture seule et elle correspond aux paramètres du premier journal de suivi. L'événement est journalisé et transmis au `read-only-bucket` par le journal de suivi.
5. L'opération API `TerminateInstances` est un événement en écriture seule et elle correspond aux paramètres du deuxième journal de suivi. L'événement est journalisé et livré au par le journal de suivi `write-only-bucket`.

Enregistrement des événements liés aux données à l'aide du AWS Management Console

Les procédures suivantes décrivent comment mettre à jour un magasin de données d'événement ou un journal de suivi existant pour journaliser les événements de données à l'aide l' AWS Management Console. Pour plus d'informations sur la création d'un magasin de données d'événement pour journaliser des événements de données, veuillez consulter Création d'un magasin de données d' CloudTrailévénements pour les événements à l'aide de la console. Pour en savoir plus sur la création d'un journal de suivi pour journaliser des événements de données, veuillez consulter Créer un journal de suivi dans la console.

Pour les sentiers, les étapes de journalisation des événements liés aux données varient selon que vous utilisez des sélecteurs d'événements avancés ou des sélecteurs d'événements de base. Vous pouvez enregistrer les événements de données pour tous les types d'événements de données à l'aide de sélecteurs d'événements avancés, mais si vous utilisez des sélecteurs d'événements de base, vous êtes limité à la journalisation des événements de données pour les compartiments Amazon S3 et les objets de compartiment, les AWS Lambda fonctions et les tables Amazon DynamoDB.

Mettre à jour un magasin de données d'événements existant pour consigner les événements de données dans AWS Management Console

Utilisez la procédure suivante pour mettre à jour un magasin de données d'événement existant afin de journaliser les événements de données. Pour plus d'informations sur l'utilisation des sélecteurs d'événements avancés, consultez Filtrer les événements liés aux données à l'aide de sélecteurs d'événements avancés cette rubrique.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, sous Lake, choisissez Entrepôts de données d'événement.

3. Sur la page Entrepôts de données d'événement, choisissez l'entrepôt de données d'événement que vous souhaitez mettre à jour.

> **Note**
>
> Vous ne pouvez activer les événements de données que dans les magasins de données d'événements qui contiennent des CloudTrail événements. Vous ne pouvez pas activer les événements de données dans les magasins de données d'événements pour les éléments de AWS Config configuration, les événements CloudTrail Insights ou les AWS non-événements. CloudTrail

4. Sur la page de détails, dans Événements de données, choisissez Modifier.
5. Si vous ne journalisez pas déjà les événements de données, choisissez la case à cocher Événements de données.
6. Pour Data event type (Type d'événement de données), choisissez le type de ressource sur lequel vous souhaitez journaliser les événements de données.
7. Choisissez un modèle de sélecteur de journaux. CloudTrail inclut des modèles prédéfinis qui enregistrent tous les événements de données pour le type de ressource. Pour créer un modèle de sélecteur de journal personnalisé, choisissez Personnaliser.
8. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.
9. Dans Sélecteurs d'événements avancés, créez une expression pour les ressources spécifiques sur lesquelles vous souhaitez journaliser les événements de données. Vous pouvez ignorer cette étape si vous utilisez un modèle de journal prédéfini.

    a. Choisissez parmi les options suivantes.

    - **`readOnly`**- `readOnly` peut être défini pour être égal à une valeur de `true` ou`false`. Les événements de données en lecture seule sont des événements qui ne modifient pas l'état d'une ressource, tels que les événements `Get*` ou `Describe*`. Les événements d'écriture ajoutent, modifient ou suppriment des ressources, des attributs ou des artefacts, tels que les événements `Put*`, `Delete*`, ou `Write*`. Pour journaliser les deux événements `read` et `write`, n'ajoutez pas de sélecteur `readOnly`.

- **`eventName`** - `eventName` peut utiliser n'importe quel opérateur. Vous pouvez l'utiliser pour inclure ou exclure tout événement de données enregistré CloudTrail, tel que `PutBucketGetItem`, ou`GetSnapshotBlock`.
- **`resources.ARN`**- Vous pouvez utiliser n'importe quel opérateur`resources.ARN`, mais si vous utilisez égal ou non, la valeur doit correspondre exactement à l'ARN d'une ressource valide du type que vous avez spécifié dans le modèle comme valeur de`resources.type`.

  Le tableau suivant affiche le format ARN valide de chaque `resources.type`.

  > **Note**
  >
  > Vous ne pouvez pas utiliser le `resources.ARN` champ pour filtrer les types de ressources dépourvus d'ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`

resources.type	resources.ARN
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-aliases/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*

resources.type	resources.ARN
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*

resources.type	resources.ARN
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Pour les tables ayant les flux activés, le champ `resources` dans l'événement de plan de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.

[2] Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante. La barre oblique de fin est intentionnelle ; ne l'excluez pas.

[3] Pour journaliser les événements sur tous les objets d'un point d'accès S3, il est recommandé d'utiliser uniquement l'ARN du point d'accès, de ne pas inclure le chemin d'accès de l'objet et d'utiliser les opérateurs `StartsWith` ou `NotStartsWith`.

Pour plus d'informations sur les formats ARN des ressources d'événements de données, consultez Actions, ressources et clés de condition dans le Guide de l'utilisateur AWS Identity and Access Management .

b. Pour chaque champ, choisissez + Conditions pour ajouter autant de conditions que vous le souhaitez, jusqu'à un maximum de 500 valeurs spécifiées pour toutes les conditions. Par exemple, pour exclure les événements de données de deux compartiments S3 des événements de données enregistrés dans votre banque de données d'événements, vous pouvez définir le champ sur Resources.ARN, définir l'opérateur pour ne commence pas par, puis coller l'ARN d'un compartiment S3 ou rechercher les compartiments S3 pour lesquels vous ne souhaitez pas enregistrer d'événements.

   Pour ajouter le deuxième compartiment S3, choisissez + Conditions, puis répétez l'instruction précédente, en collant dans l'ARN ou en recherchant un compartiment différent.

   > **Note**
   >
   > Il est possible de définir un maximum de 500 valeurs pour tous les sélecteurs d'un entrepôt de données d'événement. Cela inclut des tableaux de valeurs multiples pour un sélecteur tel que `eventName`. Si vous avez défini des valeurs uniques pour tous les sélecteurs, il est possible d'ajouter un maximum de 500 conditions à un sélecteur.

c. Choisir + champ pour ajouter des champs supplémentaires au besoin. Pour éviter les erreurs, il convient de ne pas définir de valeurs conflictuelles ou en double pour les champs. Par exemple, ne spécifiez pas un ARN dans un sélecteur pour être égal à une valeur, puis spécifiez que l'ARN n'est pas égal à la même valeur dans un autre sélecteur.

10. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Ajouter un type d'événement de données. Répétez la procédure de l'étape 6 à celle-ci pour configurer les sélecteurs d'événements avancés pour le type d'événement de données.
11. Après avoir examiné et vérifié vos choix, choisissez Enregistrer les modifications.

Mettre à jour un parcours existant pour enregistrer les événements liés aux données à l'aide de sélecteurs d'événements avancés dans le AWS Management Console

Dans le AWS Management Console, si votre parcours utilise des sélecteurs d'événements avancés, vous pouvez choisir parmi des modèles prédéfinis qui enregistrent tous les événements de données sur une ressource sélectionnée. Après avoir choisi un modèle de sélecteur de journal, il est possible de personnaliser le modèle de manière à inclure uniquement les événements de données que vous souhaitez voir le plus. Pour plus d'informations sur l'utilisation des sélecteurs d'événements avancés, consultez Filtrer les événements liés aux données à l'aide de sélecteurs d'événements avancés cette rubrique.

1. Sur les pages Tableau de bord ou Trails de la CloudTrail console, choisissez le parcours que vous souhaitez mettre à jour.
2. Sur la page de détails, dans Événements de données, choisissez Modifier.
3. Si vous ne journalisez pas déjà les événements de données, choisissez la case à cocher Événements de données.
4. Pour Data event type (Type d'événement de données), choisissez le type de ressource sur lequel vous souhaitez journaliser les événements de données.
5. Choisissez un modèle de sélecteur de journaux. CloudTrail inclut des modèles prédéfinis qui enregistrent tous les événements de données pour le type de ressource. Pour créer un modèle de sélecteur de journal personnalisé, choisissez Personnaliser.

> **Note**
>
> Le choix d'un modèle prédéfini pour les compartiments S3 permet de consigner les événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois le suivi terminé. Il permet également de consigner l'activité liée aux événements de données effectuée par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
> Si le journal de suivi s'applique à une seule région, le fait de choisir un modèle prédéfini qui journalise tous les compartiments S3 permet la journalisation des événements de données pour tous les compartiments situés dans la même région que votre journal de suivi et tous les compartiments que vous créerez ultérieurement dans cette région. Les événements de données relatifs aux compartiments Amazon S3 situés dans d'autres régions ne seront pas enregistrés dans votre AWS compte.

Si vous créez un suivi pour toutes les régions, le choix d'un modèle prédéfini pour les fonctions Lambda permet de consigner les événements de données pour toutes les fonctions actuellement présentes dans votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans n'importe quelle région une fois le suivi créé. Si vous créez un parcours pour une seule région (pour les sentiers, cela ne peut être fait qu'en utilisant le AWS CLI), cette sélection active l'enregistrement des événements de données pour toutes les fonctions actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une fois que vous aurez fini de créer le parcours. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions.
La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectués par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

6. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.
7. Dans Sélecteurs d'événements avancés, créez une expression pour les ressources spécifiques sur lesquelles vous souhaitez journaliser les événements de données. Vous pouvez ignorer cette étape si vous utilisez un modèle de journal prédéfini.

   a. Choisissez parmi les options suivantes.

   - **`readOnly`**- `readOnly` peut être défini pour être égal à une valeur de `true` ou`false`. Les événements de données en lecture seule sont des événements qui ne modifient pas l'état d'une ressource, tels que les événements `Get*` ou `Describe*`. Les événements d'écriture ajoutent, modifient ou suppriment des ressources, des attributs ou des artefacts, tels que les événements `Put*`, `Delete*`, ou `Write*`. Pour journaliser les deux événements `read` et `write`, n'ajoutez pas de sélecteur `readOnly`.
   - **`eventName`** - `eventName` peut utiliser n'importe quel opérateur. Vous pouvez l'utiliser pour inclure ou exclure tout événement de données enregistré CloudTrail, tel que `PutBucketGetItem`, ou`GetSnapshotBlock`.

- **`resources.ARN`**- Vous pouvez utiliser n'importe quel opérateur`resources.`ARN, mais si vous utilisez égal ou non, la valeur doit correspondre exactement à l'ARN d'une ressource valide du type que vous avez spécifié dans le modèle comme valeur de`resources.type`.

  Le tableau suivant affiche le format ARN valide de chaque `resources.type`.

  > **Note**
  >
  > Vous ne pouvez pas utiliser le `resources.`ARN champ pour filtrer les types de ressources dépourvus d'ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	resources.ARN
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
`AWS::Timestream::Database`	`arn:partition :timestream: region:account_ID :database/ database_name`
`AWS::Timestream::Table`	`arn:partition :timestream: region:account_ID :database/ database_name /table/table_name`
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Pour les tables ayant les flux activés, le champ `resources` dans l'événement de plan de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.

[2] Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante. La barre oblique de fin est intentionnelle ; ne l'excluez pas.

[3] Pour journaliser les événements sur tous les objets d'un point d'accès S3, il est recommandé d'utiliser uniquement l'ARN du point d'accès, de ne pas inclure le chemin d'accès de l'objet et d'utiliser les opérateurs `StartsWith` ou `NotStartsWith`.

Pour plus d'informations sur les formats ARN des ressources d'événements de données, consultez Actions, ressources et clés de condition dans le Guide de l'utilisateur AWS Identity and Access Management .

b. Pour chaque champ, choisissez + Conditions pour ajouter autant de conditions que vous le souhaitez, jusqu'à un maximum de 500 valeurs spécifiées pour toutes les conditions. Par exemple, pour exclure les événements de données de deux compartiments S3 des

événements de données enregistrés sur votre parcours, vous pouvez définir le champ sur Resources.ARN, définir l'opérateur pour ne commence pas par, puis coller l'ARN d'un compartiment S3 ou rechercher les compartiments S3 pour lesquels vous ne souhaitez pas enregistrer d'événements.

Pour ajouter le deuxième compartiment S3, choisissez + Conditions, puis répétez l'instruction précédente, en collant dans l'ARN ou en recherchant un compartiment différent.

> **Note**
>
> Il est possible de définir un maximum de 500 valeurs pour tous les sélecteurs d'un journal de suivi. Cela inclut des tableaux de valeurs multiples pour un sélecteur tel que `eventName`. Si vous avez défini des valeurs uniques pour tous les sélecteurs, il est possible d'ajouter un maximum de 500 conditions à un sélecteur.

c. Choisir + champ pour ajouter des champs supplémentaires au besoin. Pour éviter les erreurs, il convient de ne pas définir de valeurs conflictuelles ou en double pour les champs. Par exemple, ne spécifiez pas un ARN dans un sélecteur pour être égal à une valeur, puis spécifiez que l'ARN n'est pas égal à la même valeur dans un autre sélecteur.

8. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données). Répétez les étapes de 4 à cette étape pour configurer les sélecteurs d'événements avancés pour le type d'événement de données.
9. Après avoir examiné et vérifié vos choix, choisissez Enregistrer les modifications.

Mettez à jour un parcours existant pour enregistrer les événements liés aux données à l'aide des sélecteurs d'événements de base dans le AWS Management Console

Utilisez la procédure suivante pour mettre à jour un journal de suivi existant afin de journaliser des événements de données à l'aide de sélecteurs d'événements de base.

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Ouvrez la page Pistes de la CloudTrail console et choisissez le nom de la piste.

> **Note**
>
> Bien que vous puissiez modifier un journal de suivi existant pour journaliser des événements de données, les bonnes pratiques consistent à envisager la création d'un journal de suivi distinct, spécifiquement destiné à la journalisation des événements de données.

3. Pour Événements de données, choisissez Modifier.
4. Pour les compartiments Amazon S3 :
   a. Pour Data event source (Source d'événements de données), choisissez S3.
   b. Il est possible de choisir de journaliser Tous les compartiments S3 actuels et futurs ou de spécifier des compartiments ou fonctions individuels. Par défaut, les événements de données sont journalisés pour tous les compartiments S3 actuels et futurs.

      > **Note**
      >
      > Le maintien de l'option par défaut Tous les compartiments S3 actuels et futurs active la journalisation des événements de données pour tous les compartiments actuellement présents dans votre AWS compte et pour tous les compartiments que vous créez une fois que vous avez terminé de créer le journal. Il permet également de consigner l'activité liée aux événements de données effectuée par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur un bucket appartenant à un autre AWS compte.
      > Si vous créez un parcours pour une seule région (à l'aide du AWS CLI), la sélection de l'option Sélectionner tous les compartiments S3 dans votre compte permet d'enregistrer les événements de données pour tous les compartiments de la même région que votre parcours et pour tous les compartiments que vous créerez ultérieurement dans cette région. Les événements de données relatifs aux compartiments Amazon S3 situés dans d'autres régions ne seront pas enregistrés dans votre AWS compte.

   c. Si vous laissez l'option par défaut, Tous les compartiments S3 actuels et futurs, choisissez de journaliser les événements de lecture, les événements d'écriture, ou les deux.
   d. Pour sélectionner des compartiments individuels, il convient de vider les boîtes de dialogue Lecture et Écriture pour Tous les compartiments S3 actuels et futurs. Dans Sélection

du compartiment individuel, recherchez un compartiment sur lequel journaliser les événements de données. Pour rechercher des compartiments spécifiques, tapez un préfixe de compartiment pour le compartiment souhaité. Il est possible de sélectionner plusieurs compartiments dans cette fenêtre. Choisissez Ajouter un compartiment pour journaliser les événements de données pour d'autres compartiments. Choisissez de journaliser les événements Lecture tels que `GetObject`, les événements Écriture tels que `PutObject`, ou les deux.

Ce paramètre est prioritaire par rapport aux paramètres que vous définissez pour les compartiments individuels. Par exemple, si vous spécifiez la journalisation des événements Read (Lecture) pour tous les compartiments S3, puis choisissez d'ajouter un compartiment spécifique pour la journalisation des événements de données, Read (Lecture) est déjà sélectionné pour le compartiment que vous avez ajouté. Vous ne pouvez pas effacer la sélection. Vous pouvez uniquement configurer l'option pour Écriture.

Pour supprimer un compartiment de la journalisation, choisissez X.

5. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données).
6. Pour les fonctions Lambda :

   a. Pour Data event source (Source d'événement de données), choisissez Lambda.

   b. Dans Fonction Lambda, choisissez Toutes les régions pour journaliser toutes les fonctions Lambda, ou Fonction d'entrée en tant qu'ARN, pour consigner les événements de données sur une fonction spécifique.

   Pour consigner les événements de données de toutes les fonctions Lambda de votre compte AWS , sélectionnez Journaliser toutes les fonctions actuelles et futures. Ce paramètre est prioritaire par rapport aux paramètres que vous définissez pour les fonctions individuelles. Toutes les fonctions sont journalisées, même si elles ne sont pas toutes affichées.

   > **Note**
   >
   > Si vous créez un journal de suivi pour toutes les régions, cette sélection active la journalisation des événements de données pour toutes les fonctions se trouvant actuellement dans votre compte AWS et pour toute fonction Lambda que vous êtes susceptible de créer dans n'importe quelle région après avoir achevé la création du journal de suivi. Si vous créez un suivi pour une seule région (en utilisant le AWS

CLI), cette sélection active l'enregistrement des événements de données pour toutes les fonctions actuellement présentes dans cette région sur votre AWS compte, ainsi que pour toutes les fonctions Lambda que vous pourriez créer dans cette région une fois que vous aurez fini de créer le journal. Cela n'active pas la journalisation des événements de données pour les fonctions Lambda créées dans d'autres régions. La journalisation des événements de données pour toutes les fonctions permet également de consigner l'activité des événements de données effectués par n'importe quel utilisateur ou rôle dans votre AWS compte, même si cette activité est effectuée sur une fonction appartenant à un autre AWS compte.

c. Si vous choisissez Fonction d'entrée en tant qu'ARN, saisissez l'ARN d'une fonction Lambda.

> **Note**
>
> Si votre compte compte compte plus de 15 000 fonctions Lambda, vous ne pouvez pas afficher ou sélectionner toutes les fonctions dans la CloudTrail console lors de la création d'un journal. Vous pouvez toujours sélectionner l'option de journalisation de toutes les fonctions, même si elles ne sont pas affichées. Si vous souhaitez journaliser les événements de données de fonctions spécifiques, vous pouvez ajouter manuellement une fonction si vous connaissez son ARN. Vous pouvez également terminer la création du journal dans la console, puis utiliser la put-event-selectors commande AWS CLI et pour configurer la journalisation des événements de données pour des fonctions Lambda spécifiques. Pour plus d'informations, consultez Gérer les sentiers à l'aide du AWS CLI.

7. Pour ajouter un autre type de données sur lequel journaliser les événements de données, choisissez Add data event type (Ajouter un type d'événement de données).
8. Pour les tables DynamoDB :

   a. Pour Data event source (Source d'événement de données), choisissez DynamoDB.

   b. Dans Sélection d'une table DynamoDB, choisissez Parcourir pour sélectionner une table ou coller dans l'ARN d'une table DynamoDB à laquelle vous avez accès. Un ARN de table DynamoDB utilise le format suivant :

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Pour ajouter une autre table, choisissez Ajouter une ligne, puis recherchez un tableau ou collez dans l'ARN d'une table à laquelle vous avez accès.

9. Sélectionnez Enregistrer les modifications.

Enregistrement des événements liés aux données à l'aide du AWS Command Line Interface

Vous pouvez configurer vos journaux de suivi ou vos entrepôts de données d'événement de manière à ce qu'ils journalisent les événements de gestion et de données à l'aide de l' AWS CLI.

Rubriques

Enregistrement des événements liés aux données pour les sentiers à l'aide du AWS CLI

Vous pouvez configurer vos journaux de suivi de manière à ce qu'ils journalisent les événements de gestion et de données à l'aide de l' AWS CLI.

> **Note**
>
> - Sachez que si votre compte journalise plus d'une copie des événements de gestion, vous engagez des frais. Des frais sont toujours imputés pour la journalisation des événements de données. Pour plus d'informations, consultez AWS CloudTrail Tarification.
> - Vous pouvez utiliser des sélecteurs d'événements avancés ou des sélecteurs d'événements de base, mais pas les deux. Si vous appliquez des sélecteurs d'événements avancés à un journal de suivi, tous les sélecteurs d'événements de base existants sont remplacés.
> - Si votre journal de suivi utilise des sélecteurs d'événements de base, vous ne pouvez enregistrer que les types de ressources suivants :
>   - `AWS::DynamoDB::Table`
>   - `AWS::Lambda::Function`

- `AWS::S3::Object`

  Afin de journaliser des types de ressources supplémentaires, vous devez utiliser des sélecteurs d'événements avancés. Pour convertir un journal de suivi en sélecteurs d'événements avancés, exécutez la commande get-event-selectors pour confirmer les sélecteurs d'événements actuels, puis configurez les sélecteurs d'événements avancés pour qu'ils correspondent à la couverture des sélecteurs d'événements précédents, puis ajoutez des sélecteurs pour tous les types de ressources pour lesquels vous souhaitez enregistrer des événements de données.

- Vous pouvez utiliser des sélecteurs d'événements avancés pour filtrer en fonction de la valeur des champs `eventName`, `resources.ARN` et `readOnly`, ce qui vous permet de n'enregistrer que les événements de données qui vous intéressent. Pour plus d'informations sur la configuration de ces champs, consultez AdvancedFieldSelectorla référence de l'AWS CloudTrail API et Filtrer les événements liés aux données à l'aide de sélecteurs d'événements avancés cette rubrique.

Pour vérifier que votre journal de suivi journalise effectivement les événements de gestion et de données, veuillez exécuter la commande `get-event-selectors`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

La commande renvoie les sélecteurs d'événements pour le parcours.

Rubriques

- Journaliser les événements à l'aide de sélecteurs d'événements avancés
- Enregistrez tous les événements Amazon S3 pour un compartiment Amazon S3 à l'aide de sélecteurs d'événements avancés
- Journaliser Amazon S3 sur les événements AWS Outposts à l'aide de sélecteurs d'événements avancés
- Journaliser les événements à l'aide de sélecteurs d'événements de base

Journaliser les événements à l'aide de sélecteurs d'événements avancés

> **Note**
>
> Si vous appliquez des sélecteurs d'événements avancés à un journal de suivi, tous les sélecteurs d'événements de base existants sont remplacés. Avant de configurer les sélecteurs d'événements avancés, exécutez la commande get-event-selectors pour confirmer les sélecteurs d'événements actuels, puis configurez les sélecteurs d'événements avancés pour qu'ils correspondent à la couverture des sélecteurs d'événements précédents, puis ajoutez des sélecteurs pour tous les événements de données supplémentaires que vous souhaitez enregistrer.

L'exemple suivant crée des sélecteurs d'événements avancés personnalisés pour un journal nommé de manière *TrailName* à inclure les événements de gestion de lecture et d'écriture (en omettant le `readOnly` sélecteur) et les événements de `DeleteObject` données pour toutes les combinaisons de compartiments `PutObject` et de préfixes Amazon S3, à l'exception d'un bucket nommé `sample_bucket_name` et d'événements de données pour une fonction nommée. AWS Lambda `MyLambdaFunction` Comme il s'agit de sélecteurs d'événements avancés personnalisés, chaque ensemble de sélecteurs a un nom descriptif. Notez qu'une barre oblique de fin fait partie de la valeur ARN pour les compartiments S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
```

```
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

L'exemple renvoie le sélecteur d'événements avancés configuré pour le journal de suivi.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
```

```
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Enregistrez tous les événements Amazon S3 pour un compartiment Amazon S3 à l'aide de sélecteurs d'événements avancés

> **Note**
>
> Si vous appliquez des sélecteurs d'événements avancés à un journal de suivi, tous les sélecteurs d'événements de base existants sont remplacés.

L'exemple suivant indique comment configurer votre journal de suivi pour inclure tous les événements de données pour tous les objets Amazon S3 dans un compartiment S3 spécifique. La valeur des événements S3 pour le champ `resources.type` est `AWS::S3::Object`. Étant donné que les valeurs ARN pour les objets S3 et les compartiments S3 sont légèrement différentes, il convient d'ajouter l'opérateur `StartsWith` pour `resources.ARN` afin de capturer tous les événements.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
```

```
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

La commande renvoie l'exemple de résultat suivant:

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                }
            ]
        }
    ]
}
```

Journaliser Amazon S3 sur les événements AWS Outposts à l'aide de sélecteurs d'événements avancés

> **Note**
>
> Si vous appliquez des sélecteurs d'événements avancés à un journal de suivi, tous les sélecteurs d'événements de base existants sont remplacés.

L'exemple suivant indique comment configurer votre journal de suivi pour inclure tous les événements de données pour tous les Amazon S3 sur les objets Outposts dans votre avant-poste.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

La commande renvoie l'exemple de résultat suivant.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
```

```
                    ]
                }
            ]
        }
    ]
}
```

Journaliser les événements à l'aide de sélecteurs d'événements de base

Voici un exemple de résultat de la commande get-event-selectors affichant les sélecteurs d'événements de base. Par défaut, lorsque vous créez un suivi à l'aide du AWS CLI, un journal enregistre tous les événements de gestion. Par défaut, les journaux de suivi ne journalisent pas les événements de données.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

Pour configurer votre journal de suivi de manière à ce qu'il journalise les événements de gestion et de données, veuillez exécuter la commande put-event-selectors.

L'exemple suivant montre comment utiliser des sélecteurs d'événements de base pour configurer votre suivi afin d'inclure tous les événements de gestion et de données pour les objets S3 dans deux préfixes de compartiment S3. Vous pouvez spécifier de 1 à 5 sélecteurs d'événements pour un journal de suivi. Vous pouvez spécifier de 1 à 250 ressources de données pour un journal de suivi.

> **Note**
>
> Le nombre maximal de ressources de données S3 est 250, si vous choisissez de limiter les événements de données à l'aide de sélecteurs d'événements de base.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
```

```
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

La commande renvoie les sélecteurs d'événements configurés pour le journal de suivi.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

Enregistrement des événements de données pour les magasins de données d'événements à l'aide du AWS CLI

Vous pouvez configurer vos magasins de données d'événement de manière à ce qu'ils journalisent les événements de gestion et de données à l'aide de l' AWS CLI. Utilisez la commande `create-event-data-store` pour créer un entrepôt de données d'événement afin de journaliser les événements de données. Utilisez la commande `update-event-data-store` pour mettre à jour les sélecteurs d'événements avancés pour un entrepôt de données d'événement existant.

Pour savoir si votre entrepôt de données d'événement inclut des événements de données, exécutez la commande `get-event-data-store`.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

La commande renvoie les paramètres de l'entrepôt de données d'événement.

```
{
```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

Rubriques

- Inclure tous les événements Amazon S3 pour un compartiment
- Inclure Amazon S3 dans les événements AWS Outposts

Inclure tous les événements Amazon S3 pour un compartiment

L'exemple suivant montre comment créer un entrepôt de données d'événements pour inclure tous les événements de données pour tous les objets Amazon S3 dans un compartiment S3 spécifique. La valeur des événements S3 pour le champ `resources.type` est `AWS::S3::Object`. Étant

donné que les valeurs ARN pour les objets S3 et les compartiments S3 sont légèrement différentes, il convient d'ajouter l'opérateur `StartsWith` pour `resources.ARN` afin de capturer tous les événements.

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

La commande renvoie l'exemple de résultat suivant:

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                },
                {
```

```
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

Inclure Amazon S3 dans les événements AWS Outposts

L'exemple suivant montre comment créer un entrepôt de données d'événements qui inclut tous les événements de données pour tous les Amazon S3 sur les objets Outposts dans votre avant-poste.

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

La commande renvoie l'exemple de résultat suivant.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
```

```
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

Filtrer les événements liés aux données à l'aide de sélecteurs d'événements avancés

Cette section décrit comment utiliser les sélecteurs d'événements avancés pour créer des sélecteurs précis, qui vous aident à contrôler les coûts en enregistrant uniquement les événements de données spécifiques qui vous intéressent.

Par exemple :

- Vous pouvez inclure ou exclure des appels d'API spécifiques en ajoutant un filtre sur le `eventName` champ.
- Vous pouvez inclure ou exclure la journalisation pour des ressources spécifiques en ajoutant un filtre sur le `resources.ARN` champ. Par exemple, si vous enregistrez des événements de données S3, vous pouvez exclure la journalisation du compartiment S3 de votre parcours.

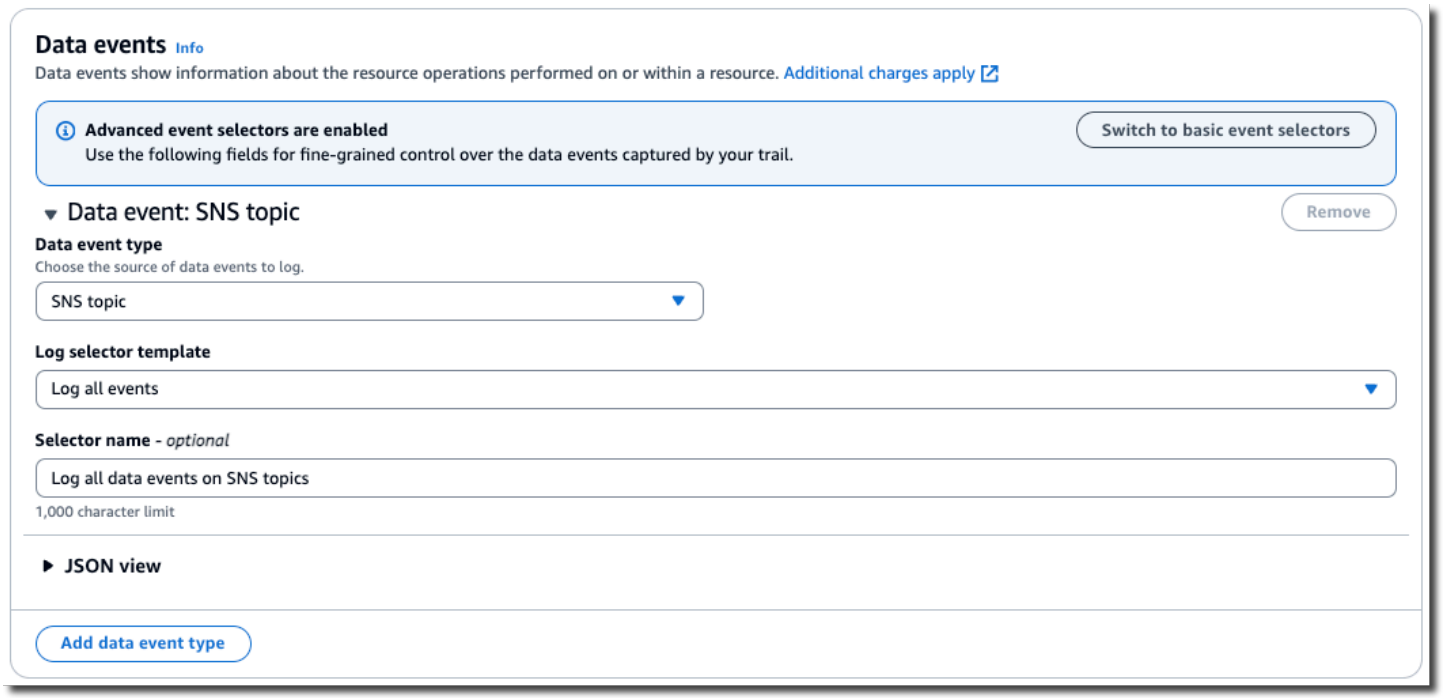
- Vous pouvez choisir de ne consigner que les événements en écriture seule ou en lecture seule en ajoutant un filtre sur le champ. `readOnly`

Le tableau suivant fournit des informations supplémentaires sur les champs configurables pour les sélecteurs d'événements avancés.

Champ	Obligatoire	Opérateurs valides	Description
`eventCategory`	Oui	`Equals`	Ce champ est configuré pour enregistrer `Data` les événements liés aux données.
`resources.type`	Oui	`Equals`	Ce champ est utilisé pour sélectionner le type de ressource pour lequel vous souhaitez enregistrer des événements de données. Le tableau des événements de données indique les valeurs possibles.
`readOnly`	Non	`Equals`	Il s'agit d'un champ facultatif utilisé pour inclure ou exclure des événements de données en fonction de la `readOnly` valeur. Une valeur des `true` journaux ne lit que les événements. Une valeur de `false` logs n'écrit que des événements. Si vous n'ajoutez pas ce champ, CloudTrail enregistre les événements de lecture et d'écriture.
`eventName`	Non	N'importe quel compte	Il s'agit d'un champ facultatif utilisé pour filtrer ou filtrer tout événement de données enregistré CloudTrail, tel que ou. `PutBucket` `GetSnapshotBlock` Si vous utilisez le AWS CLI, vous pouvez spécifier plusieurs valeurs en séparant chaque valeur par une virgule. Si vous utilisez la console, vous pouvez spécifier plusieurs valeurs en créant une

Champ	Obligatoire	Opérateurs valides	Description
			condition pour chacune des valeurs que `eventName` vous souhaitez filtrer.
`resources.ARN`	Non	N'importe quel compte	Il s'agit d'un champ facultatif utilisé pour exclure ou inclure des événements de données pour une ressource spécifique en fournissant le`resources.ARN` . Vous pouvez utiliser n'importe quel opérateur`resources.ARN` , mais si vous utilisez `Equals` ou`NotEquals` , la valeur doit correspondre exactement à l'ARN d'une ressource valide pour celle que `resoureces.type` vous avez spécifiée. Si vous utilisez le AWS CLI, vous pouvez spécifier plusieurs valeurs en séparant chaque valeur par une virgule. Si vous utilisez la console, vous pouvez spécifier plusieurs valeurs en créant une condition pour chacune des valeurs que `resources.ARN` vous souhaitez filtrer.

Pour enregistrer les événements de données à l'aide de la CloudTrail console, vous choisissez l'option Événements de données, puis sélectionnez le type d'événement de données qui vous intéresse lorsque vous créez ou mettez à jour un journal ou un magasin de données d'événements. Le tableau des événements de données indique les types d'événements de données possibles que vous pouvez choisir sur la CloudTrail console.



Pour enregistrer des événements de données avec le AWS CLI, configurez le `--advanced-event-selector` paramètre pour définir la valeur `eventCategory` égale `Data` et la `resources.type` valeur égale à la valeur du type de ressource pour lequel vous souhaitez enregistrer les événements de données. Le tableau des événements de données répertorie les types de ressources disponibles.

Par exemple, si vous souhaitez enregistrer les événements de données pour tous les pools Cognito Identity, vous devez configurer le `--advanced-event-selectors` paramètre comme suit :

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
     }
]'
```

L'exemple précédent enregistre tous les événements de données Cognito sur les groupes d'identités. Vous pouvez affiner davantage les sélecteurs d'événements avancés pour filtrer les `eventName``readOnly`, et les `resources.`ARN champs pour enregistrer des événements spécifiques présentant un intérêt ou exclure des événements qui ne présentent aucun intérêt.

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les événements de données en fonction de plusieurs conditions. Par exemple, vous pouvez configurer des sélecteurs d'événements avancés pour consigner tous les appels Amazon S3 `PutObject` et `DeleteObject` API, mais exclure la journalisation des événements pour un compartiment S3 spécifique, comme illustré dans l'exemple suivant.

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
]'
```

Vous pouvez utiliser des sélecteurs d'événements avancés pour consigner à la fois les événements de gestion et de données. Pour enregistrer des événements de données pour plusieurs types de ressources, ajoutez une instruction de sélection de champs pour chaque type de ressource pour lequel vous souhaitez enregistrer des événements de données.

> **Note**
>
> Les sentiers peuvent utiliser des sélecteurs d'événements de base ou des sélecteurs d'événements avancés, mais pas les deux. Si vous appliquez des sélecteurs d'événements avancés à un journal de suivi, tous les sélecteurs d'événements de base existants sont remplacés.

Rubriques

- Filtrer les événements de données par eventName
- Filtrer les événements de données par resources.ARN
- Filtrer les événements de données par readOnly valeur

Filtrer les événements de données par **eventName**

À l'aide de sélecteurs d'événements avancés, vous pouvez inclure ou exclure des événements en fonction de la valeur du `eventName` champ. Le filtrage sur le `eventName` peut aider à contrôler les coûts, car vous évitez d'encourir des coûts lorsque Service AWS vous enregistrez des événements de données ajoute la prise en charge de nouvelles API de données.

Vous pouvez utiliser n'importe quel opérateur avec le `eventName` champ. Vous pouvez l'utiliser pour filtrer ou filtrer tout événement de données enregistré CloudTrail, tel que ou. `PutBucket` `GetSnapshotBlock`

Rubriques

- Filtrer les événements liés aux données à eventName l'aide du AWS Management Console
- Filtrer les événements liés aux données à eventName l'aide du AWS CLI

Filtrer les événements liés aux données à **eventName** l'aide du AWS Management Console

Procédez comme suit pour filtrer sur le `eventName` terrain à l'aide de la CloudTrail console.

1. Suivez les étapes de la procédure de création d'un journal ou suivez les étapes de la procédure de création d'un magasin de données d'événements.
2. Au fur et à mesure que vous suivez les étapes de création du magasin de données de parcours ou d'événement, effectuez les sélections suivantes :

   a. Choisissez Data events.

   b. Choisissez le type d'événement de données pour lequel vous souhaitez enregistrer les événements de données.

   c. Pour le modèle de sélecteur de journal, choisissez Personnalisé.

   d. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.

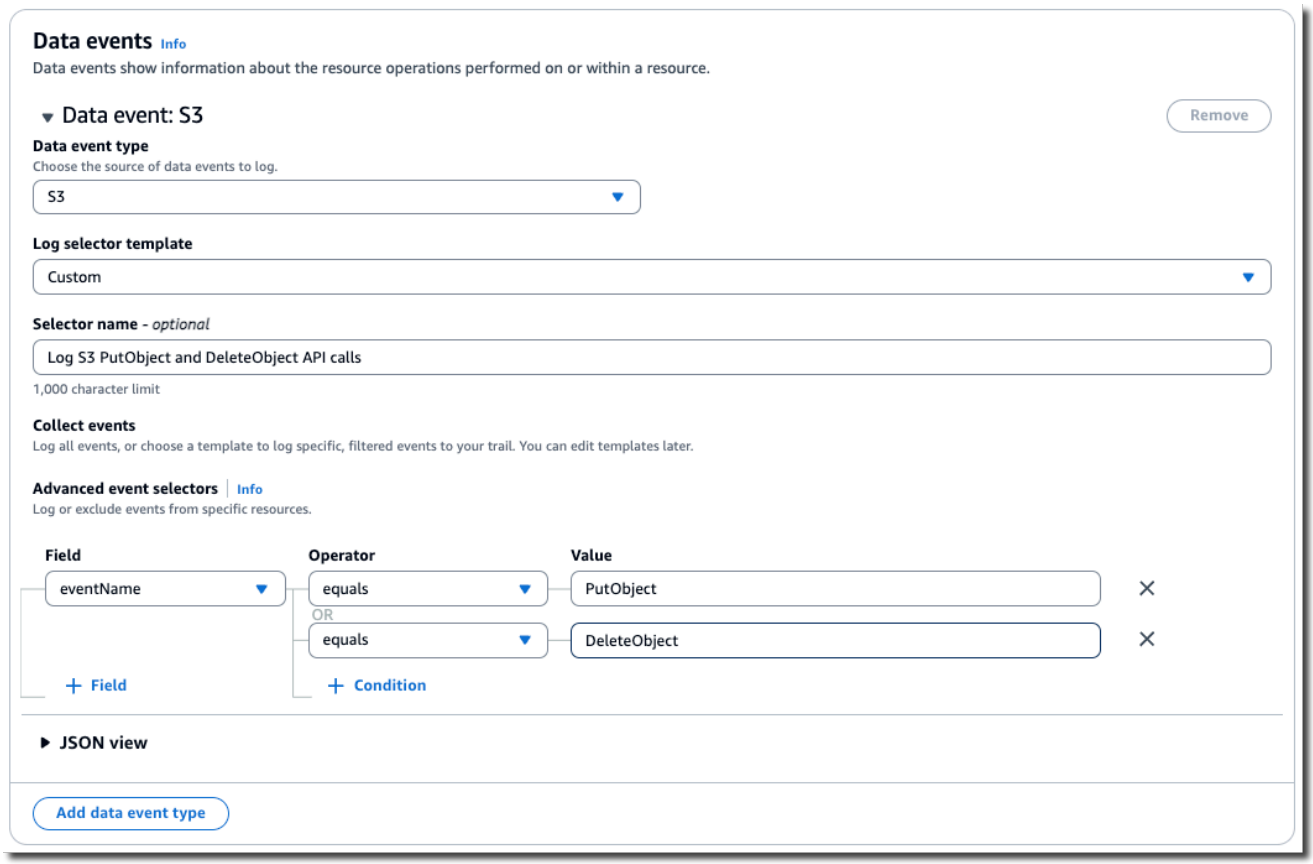
   e. Dans les sélecteurs d'événements avancés, procédez comme suit pour filtrer les `eventName` éléments suivants :

      i. Pour Field, choisissez EventName.

ii. Pour Opérateur, choisissez l'opérateur de condition. Dans cet exemple, nous allons choisir equals parce que nous voulons enregistrer un appel d'API spécifique.

iii. Dans Valeur, entrez le nom de l'événement sur lequel vous souhaitez filtrer.

iv. Pour filtrer sur une autre option`eventName`, choisissez + Condition.



f. Choisissez +Champ pour ajouter des filtres sur d'autres champs.

Filtrer les événements liés aux données à **`eventName`** l'aide du AWS CLI

À l'aide du AWS CLI, vous pouvez filtrer le `eventName` champ pour inclure ou exclure des événements spécifiques.

L'exemple suivant enregistre les événements de données S3 sur un parcours. Ils `--advanced-event-selectors` sont configurés pour enregistrer uniquement les événements de données pour les appels `GetObject``PutObject`, et `DeleteObject` API.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
```

```
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
  }
]'
```

L'exemple suivant crée un nouveau magasin de données d'événements qui enregistre les événements de données pour les API EBS Direct mais exclut les appels `ListChangedBlocks` d'API. Vous pouvez utiliser la update-event-data-storecommande pour mettre à jour un magasin de données d'événements existant.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
         ]
    }
]'
```

Filtrer les événements de données par **`resources.ARN`**

À l'aide de sélecteurs d'événements avancés, vous pouvez filtrer en fonction de la valeur du `resources.ARN` champ.

Vous pouvez utiliser n'importe quel opérateur`resources.ARN`, mais si vous utilisez `Equals` ou`NotEquals`, la valeur doit correspondre exactement à l'ARN d'une ressource valide pour la `resources.type` valeur que vous avez spécifiée. Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante.

Le tableau suivant affiche le format ARN valide de chaque `resources.type`.

> **Note**
>
> Vous ne pouvez pas utiliser le `resources.ARN` champ pour filtrer les types de ressources dépourvus d'ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`
`AWS::Bedrock::AgentAlias`	`arn:partition :bedrock: region:account_ID :agent-alias/ agent_ID/alias_ID`
`AWS::Bedrock::KnowledgeBase`	`arn:partition :bedrock: region:account_ID :knowledge-base/knowledge_base_ID`

resources.type	resources.ARN
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*

resources.type	resources.ARN
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*

resources.type	resources.ARN
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*

resources.type	resources.ARN
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*

resources.type	resources.ARN
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemake r: *region*:*account_ID* :feature- group/ *feature_group_name*

resources.type	resources.ARN
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	L'ARN doit être dans l'un des formats suivants : • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Pour les tables ayant les flux activés, le champ `resources` dans l'événement de plan de données contient à la fois `AWS::DynamoDB::Stream` et `AWS::DynamoDB::Table`. Si vous spécifiez `AWS::DynamoDB::Table` comme `resources.type`, les événements de table DynamoDB et les événements de flux DynamoDB sont journalisés par défaut. Pour exclure les événements de flux, ajoutez un filtre sur le `eventName` champ.

[2] Pour journaliser tous les événements de données pour tous les objets d'un compartiment S3 spécifique, utilisez l'opérateur `StartsWith` et n'incluez que l'ARN du compartiment comme valeur correspondante. La barre oblique de fin est intentionnelle ; ne l'excluez pas.

[3] Pour journaliser les événements sur tous les objets d'un point d'accès S3, il est recommandé d'utiliser uniquement l'ARN du point d'accès, de ne pas inclure le chemin d'accès de l'objet et d'utiliser les opérateurs `StartsWith` ou `NotStartsWith`.

Rubriques

- Filtrer les événements liés aux données à resources.ARN l'aide du AWS Management Console
- Filtrer les événements liés aux données à resources.ARN l'aide du AWS CLI

Filtrer les événements liés aux données à **`resources.ARN`** l'aide du AWS Management Console

Procédez comme suit pour filtrer sur le `resources.ARN` terrain à l'aide de la CloudTrail console.

1. Suivez les étapes de la procédure de création d'un journal ou suivez les étapes de la procédure de création d'un magasin de données d'événements.
2. Au fur et à mesure que vous suivez les étapes de création du magasin de données de parcours ou d'événement, effectuez les sélections suivantes :
   a. Choisissez Data events.
   b. Choisissez le type d'événement de données pour lequel vous souhaitez enregistrer les événements de données.
   c. Pour le modèle de sélecteur de journal, choisissez Personnalisé.
   d. (Facultatif) Dans Nom du sélecteur, saisissez un nom pour identifier votre sélecteur. Le nom du sélecteur est un nom descriptif pour un sélecteur d'événements avancé, tel que « Journaliser les événements de données pour deux compartiments S3 uniquement ». Le nom du sélecteur est répertorié comme `Name` dans le sélecteur d'événements avancé et est visible si vous développez la Vue JSON.

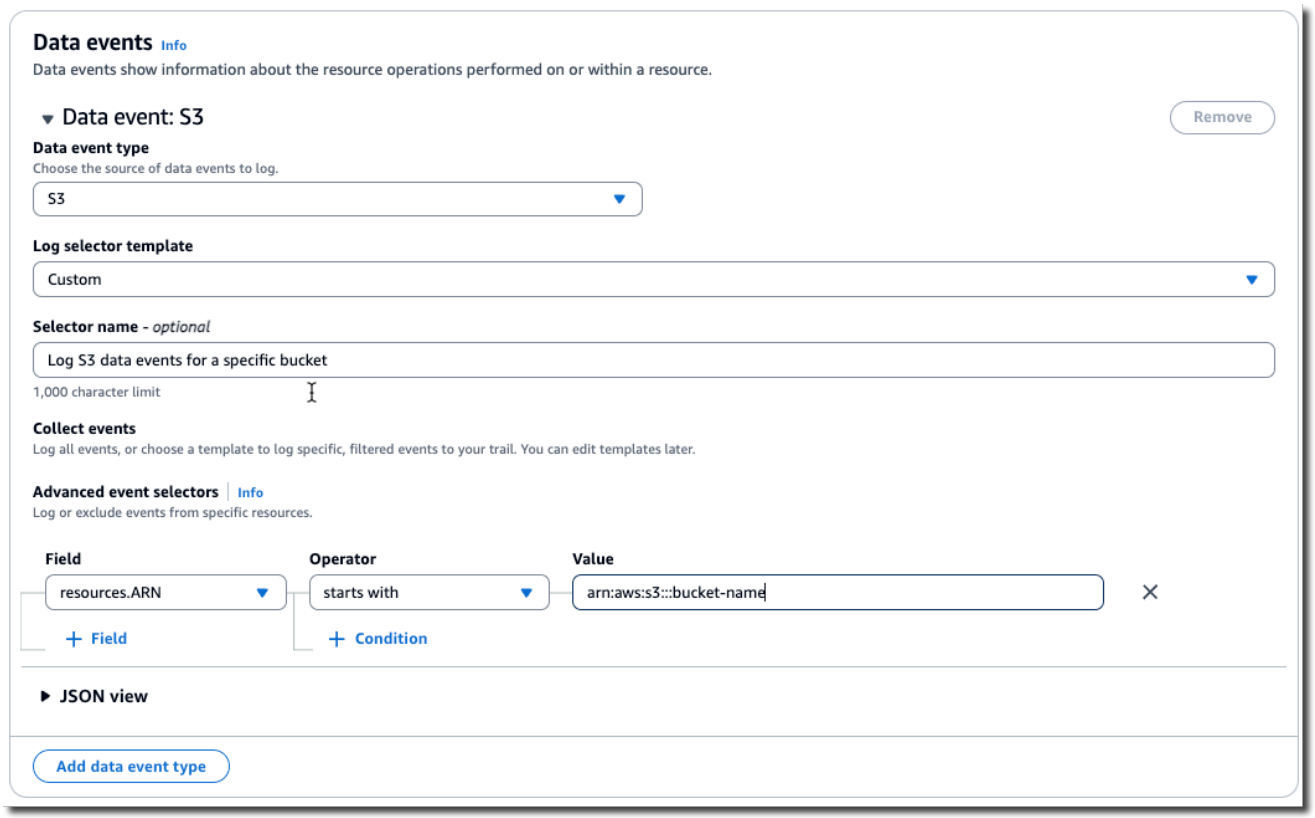
e. Dans les sélecteurs d'événements avancés, procédez comme suit pour filtrer les `resources.ARN` éléments suivants :

   i. Pour Champ, choisissez resources.ARN.

   ii. Pour Opérateur, choisissez l'opérateur de condition. Dans cet exemple, nous allons choisir commence par parce que nous voulons enregistrer les événements de données pour un compartiment S3 spécifique.

   iii. Dans Value, entrez l'ARN de votre type de ressource (par exemple, *`arn:aws:s3 : ::bucket-name`*).

   iv. Pour en filtrer un autre`resources.ARN`, choisissez + Condition.



f. Choisissez +Champ pour ajouter des filtres sur d'autres champs.

Filtrer les événements liés aux données à **`resources.ARN`** l'aide du AWS CLI

À l'aide de AWS CLI, vous pouvez filtrer le `resources.ARN` champ pour enregistrer les événements relatifs à un ARN spécifique ou exclure la journalisation pour un ARN spécifique.

L'exemple suivant indique comment configurer votre journal de suivi pour inclure tous les événements de données pour tous les objets Amazon S3 dans un compartiment S3 spécifique. La valeur des événements S3 pour le champ `resources.type` est `AWS::S3::Object`. Étant donné que les valeurs ARN pour les objets S3 et les compartiments S3 sont légèrement différentes, il convient d'ajouter l'opérateur `StartsWith` pour `resources.ARN` afin de capturer tous les événements.

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:aws:s3:::bucket_name/"] }
            ]
    }
]'
```

Filtrer les événements de données par **`readOnly`** valeur

À l'aide de sélecteurs d'événements avancés, vous pouvez filtrer en fonction de la valeur du `readOnly` champ.

Vous ne pouvez utiliser l'`Equals`opérateur qu'avec le `readOnly` champ. Vous pouvez définir la `readOnly` valeur sur `true` ou`false`. Si vous n'ajoutez pas ce champ, CloudTrail enregistre les événements de lecture et d'écriture. Une valeur des `true` journaux ne lit que les événements. Une valeur de `false` logs n'écrit que des événements.

Rubriques

- Filtrer les événements de données par readOnly valeur à l'aide du AWS Management Console
- Filtrer les événements de données par readOnly valeur à l'aide du AWS CLI

Filtrer les événements de données par **`readOnly`** valeur à l'aide du AWS Management Console

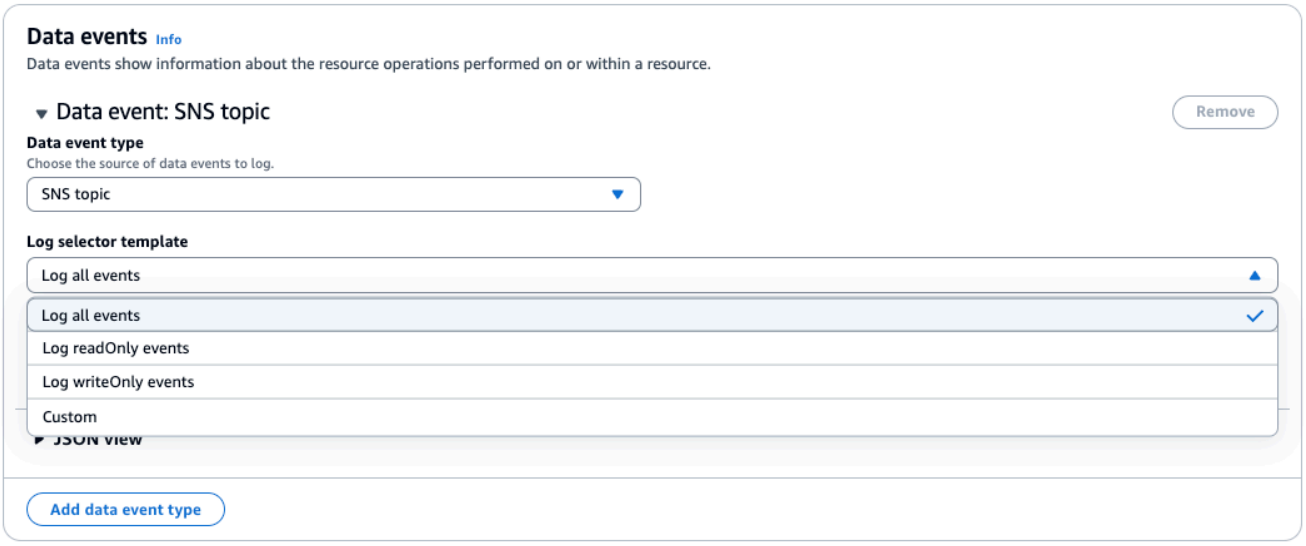
Procédez comme suit pour filtrer sur le `readOnly` terrain à l'aide de la CloudTrail console.

1. Suivez les étapes de la procédure de création d'un journal ou suivez les étapes de la procédure de création d'un magasin de données d'événements.
2. Au fur et à mesure que vous suivez les étapes de création du magasin de données de parcours ou d'événement, effectuez les sélections suivantes :

   a. Choisissez Data events.

   b. Choisissez le type d'événement de données pour lequel vous souhaitez enregistrer les événements de données.

   c. Pour le modèle de sélecteur de journal, choisissez le modèle adapté à votre cas d'utilisation.



Si vous avez l'intention de le faire	Choisissez ce modèle de sélecteur de journal
Enregistrez uniquement les événements de lecture et n'appliquez aucun autre filtre (par exemple, sur la `resources.ARN` valeur).	Enregistrer les événements en lecture seule
Consignez uniquement les événements d'écriture et n'appliquez aucun autre filtre (par exemple, sur la `resources.ARN` valeur).	Enregistrer les événements WriteOnly

Si vous avez l'intention de le faire	Choisissez ce modèle de sélecteur de journal
Filtrez sur la `readOnly` valeur et appliquez des filtres supplémentaires (par exemple, sur la `resources.ARN` valeur).	Personnalisé Dans les sélecteurs d'événements avancés, procédez comme suit pour filtrer en fonction de la `readOnly` valeur : Pour consigner les événements d'écriture a. Pour Champ, choisissez readOnly. b. Pour Opérateur, choisissez Égal à. c. Pour le champ Valeur, saisissez **`false`**. d. Choisissez +Champ pour ajouter des filtres sur d'autres champs. Pour enregistrer les événements de lecture a. Pour Champ, choisissez readOnly. b. Pour Opérateur, choisissez Égal à. c. Pour le champ Valeur, saisissez **`true`**. d. Choisissez +Champ pour ajouter des filtres sur d'autres champs.

Filtrer les événements de données par **`readOnly`** valeur à l'aide du AWS CLI

À l'aide de AWS CLI, vous pouvez filtrer sur le `readOnly` terrain.

Vous ne pouvez utiliser l'`Equals`opérateur qu'avec le `readOnly` champ. Vous pouvez définir la `readOnly` valeur sur `true` ou`false`. Si vous n'ajoutez pas ce champ, CloudTrail enregistre les événements de lecture et d'écriture. Une valeur des `true` journaux ne lit que les événements. Une valeur de `false` logs n'écrit que des événements.

L'exemple suivant montre comment configurer votre journal pour consigner les événements de données en lecture seule pour tous les objets Amazon S3.

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors '[
    {
            "Name": "Log read-only S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "readOnly", "Equals": ["true"] }
            ]
    }
]'
```

L'exemple suivant crée un nouveau magasin de données d'événements qui enregistre uniquement les événements de données en écriture uniquement pour les API EBS Direct. Vous pouvez utiliser la update-event-data-storecommande pour mettre à jour un magasin de données d'événements existant.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName" \
--advanced-event-selectors \
'[
    {
            "Name": "Log write-only EBS Direct API data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
                { "Field": "readOnly", "Equals": ["false"] }
            ]
     }
]'
```

La journalisation des événements de données pour la conformité AWS Config

Si vous utilisez des packs de AWS Config conformité pour aider votre entreprise à maintenir la conformité aux normes formalisées telles que celles requises par le Federal Risk and Authorization Management Program (FedRAMP) ou le National Institute of Standards and Technology (NIST), les packs de conformité pour les cadres de conformité nécessitent généralement que vous enregistriez

les événements de données pour les compartiments Amazon S3, au minimum. Les packs de conformité pour les cadres de conformité comprennent une règle gérée appelée `cloudtrail-s3-dataevents-enabled`, qui vérifie la journalisation des événements de données S3 dans votre compte. De nombreux packs de conformité qui ne sont pas associés aux cadres de conformité nécessitent également la journalisation des événements de données S3. Voici des exemples de packs de conformité qui intègrent cette règle.

- Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected
- Bonnes pratiques de fonctionnement pour le titre 21 CFR Part 11 de la FDA
- Bonnes pratiques de fonctionnement pour FFIEC
- Bonnes pratiques de fonctionnement pour FedRAMP (modérée)
- Bonnes pratiques de fonctionnement pour la sécurité HIPAA
- Bonnes pratiques de fonctionnement pour K-ISMS
- Bonnes pratiques de fonctionnement pour la journalisation

Pour obtenir la liste complète des exemples de packs de conformité disponibles dans AWS Config, consultez la section Modèles d'exemples de packs de conformité dans le Guide du AWS Config développeur.

Enregistrement des événements liés aux données avec les AWS SDK

Exécutez l'GetEventSelectorsopération pour voir si votre parcours enregistre des événements de données. Vous pouvez configurer vos sentiers pour enregistrer les événements liés aux données en exécutant l'PutEventSelectorsopération. Pour plus d'informations, consultez la page Référence de l'API AWS CloudTrail.

Exécutez l'GetEventDataStoreopération pour voir si votre banque de données d'événements enregistre des événements de données. Vous pouvez configurer vos magasins de données d'événements pour inclure des événements de données en exécutant les UpdateEventDataStoreopérations CreateEventDataStoreor et en spécifiant des sélecteurs d'événements avancés. Pour plus d'informations, consultez les pages Créez, mettez à jour et gérez des banques de données d'événements à l'aide du AWS CLI et Référence de l'API AWS CloudTrail.

Envoi d'événements à Amazon CloudWatch Logs

CloudTrail prend en charge l'envoi d'événements de données vers CloudWatch Logs. Lorsque vous configurez votre journal pour envoyer des événements à votre groupe de CloudWatch journaux Logs,

il CloudTrail envoie uniquement les événements que vous spécifiez dans votre journal. Par exemple, si vous configurez votre journal pour enregistrer uniquement les événements liés aux données, il transmet les événements de données uniquement à votre groupe de CloudWatch journaux Logs. Pour plus d'informations, voir Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.

Journalisation des événements Insights

AWS CloudTrail Insights aide AWS les utilisateurs à identifier les activités inhabituelles associées aux appels d'API et aux taux d'erreur des API et à y répondre en analysant en permanence les événements CloudTrail de gestion. CloudTrail Insights analyse vos modèles habituels de volume d'appels d'API et de taux d'erreur d'API, également appelés référence, et génère des événements Insights lorsque le volume d'appels ou les taux d'erreur sont en dehors des modèles normaux. Les événements Insights sur le volume d'appels d'API sont générés pour les API de gestion `write`, et les événements Insights sur le taux d'erreur de l'API sont générés pour les API de gestion `read` et `write`.

> **Note**
>
> Pour enregistrer les événements Insights sur le volume d'appels d'API, le journal de suivi ou l'entrepôt de données d'événements doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, le journal de suivi ou l'entrepôt de données d'événements doit enregistrer les événements de gestion `read` ou `write`.

CloudTrail Insights analyse les événements de gestion qui se produisent dans une seule région, et non à l'échelle mondiale. Un événement CloudTrail Insights est généré dans la même région que les événements de gestion connexes.

Des frais supplémentaires s'appliquent pour les événements Insights. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations, consultez Tarification d'AWS CloudTrail.

Table des matières

Comprendre la diffusion d'événements Insights

Contrairement aux autres types d'événements qui CloudTrail capturent, les événements Insights sont enregistrés uniquement lorsque des modifications de l'utilisation de l'API de votre compte sont CloudTrail détectées, qui diffèrent considérablement des modèles d'utilisation habituels du compte.

L'endroit CloudTrail où les événements sont organisés et le temps nécessaire pour recevoir les événements Insights varient entre les sentiers et les magasins de données sur les événements.

Diffusion d'événements Insights pour les journaux de suivi

Si vous avez activé les événements Insights sur un parcours et que vous CloudTrail détectez une activité inhabituelle, CloudTrail diffuse les événements Insights dans le `/CloudTrail-Insight` dossier du compartiment S3 de destination choisi pour votre parcours. Une fois que vous avez activé CloudTrail Insights pour la première fois sur un trail, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 36 heures, si une activité inhabituelle est détectée.

Si vous désactivez la journalisation des événements Insights sur un parcours puis que vous réactivez les événements Insights, ou si vous arrêtez et redémarrez la journalisation sur un suivi, le redémarrage de la diffusion des événements Insights peut prendre jusqu' CloudTrail à 36 heures, si une activité inhabituelle est détectée.

Diffusion d'événements Insights pour les entrepôts de données d'événement

Si vous avez activé les événements Insights sur un magasin de données d'événements source, CloudTrail diffuse les événements Insights dans le magasin de données d'événements de destination. Une fois que vous avez activé CloudTrail Insights pour la première fois dans le magasin de données d'événements source, la transmission du premier événement Insights CloudTrail au magasin de données d'événements de destination peut prendre jusqu'à 7 jours, si une activité inhabituelle est détectée.

Si vous désactivez la journalisation des événements Insights dans un magasin de données d'événements source, puis que vous réactivez les événements Insights, ou que vous arrêtez et redémarrez l'ingestion d'événements dans un magasin de données d'événements source, le redémarrage de la diffusion des événements Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée. Des frais supplémentaires s'appliquent pour l'ingestion d'événements Insights à CloudTrail Lake. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Enregistrement des événements Insights à l'aide du AWS Management Console

Vous pouvez activer les événements Insights sur un journal de suivi ou un entrepôt de données d'événement à l'aide de la console.

Rubriques

- Activation CloudTrail des événements Insights sur un parcours existant
- Activation CloudTrail des événements Insights sur un magasin de données d'événements existant

Activation CloudTrail des événements Insights sur un parcours existant

Utilisez la procédure suivante pour activer les événements CloudTrail Insights sur un parcours existant. Par défaut, les événements Insights ne sont pas activés.

1. Dans le volet de navigation gauche de la CloudTrail console, ouvrez la page Sentiers et choisissez un nom de sentier.
2. Dans Insights events (Événements Insights) choisissez Edit (Modifier).

> **Note**
>
> Des frais supplémentaires s'appliquent pour la journalisation des événements Insights. Pour les CloudTrail tarifs, consultez la section AWS CloudTrail Tarification.

3. Dans Event type (Type d'événement), choisissez Insights events (Événements Insights).
4. Dans Événements Insights, sous choisissez Types Insights, choisissez Taux d'appels d'API, Taux d'erreurs d'API, ou les deux. Votre journal de suivi doit journaliser les événements de gestion Écriture pour journaliser les événements Insights afin de connaître le Taux d'appels d'API. Votre journal de suivi doit journaliser les événements de gestion Lecture ou Écriture pour journaliser les événements Insights afin de connaître le Taux d'erreur de l'API.
5. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

La diffusion des premiers événements Insights peut prendre jusqu' CloudTrail à 36 heures si une activité inhabituelle est détectée.

Activation CloudTrail des événements Insights sur un magasin de données d'événements existant

Utilisez la procédure suivante pour activer les événements CloudTrail Insights sur un magasin de données d'événements existant. Par défaut, les événements Insights ne sont pas activés.

Des frais supplémentaires s'appliquent pour l'ingestion d'événements Insights à CloudTrail Lake. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

> **Note**
>
> Vous ne pouvez activer les événements CloudTrail Insights que sur les banques de données d'événements contenant CloudTrail des événements de gestion. Vous ne pouvez pas activer CloudTrail les événements Insights sur d'autres types de banques de données d'événements.

1. Dans le volet de navigation gauche de la CloudTrail console, sous Lake, choisissez Event data stores.
2. Choisissez le nom de l'entrepôt de données d'événement.
3. Pour Événements de gestion, choisissez Modifier.
4. Choisissez Activer Insights.
5. Choisissez le magasin de données d'événements de destination dans lequel CloudTrail les événements Insights seront diffusés. L'entrepôt de données d'événement de destination collectera les événements Insights en fonction de l'activité de gestion des événements dans cet entrepôt de données d'événement. Pour plus d'informations sur la création de l'entrepôt de données événements de destination, veuillez consulter Pour créer un entrepôt de données d'événement de destination qui journalise les événements Insights.
6. Sous Choisir les types Insights, choisissez Taux d'appels d'API, Taux d'erreur de l'API, ou les deux. Votre entrepôt de données d'événement doit enregistrer les événements de gestion Écriture pour enregistrer les événements Insights afin de connaître le Taux d'appels d'API. Votre entrepôt de données d'événement doit enregistrer les événements de gestion en Lecture ou en Écriture pour enregistrer les événements Insights afin de connaître le Taux d'erreur de l'API.
7. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

La diffusion des premiers événements Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée.

Enregistrement des événements Insights à l'aide du AWS Command Line Interface

Vous pouvez configurer vos journaux de suivi ou vos entrepôts de données d'événement pour qu'ils journalisent les événements Insights à l'aide de l' AWS CLI.

> **Note**
>
> Pour enregistrer les événements Insights sur le volume d'appels d'API, le journal de suivi ou l'entrepôt de données d'événements doit enregistrer les événements de gestion `write`. Pour enregistrer les événements Insights sur le taux d'erreur de l'API, le journal de suivi ou l'entrepôt de données d'événements doit enregistrer les événements de gestion `read` ou `write`.

Rubriques

- Enregistrement des événements Insights pour un parcours à l'aide du AWS CLI
- Enregistrement des événements Insights pour une banque de données d'événements à l'aide du AWS CLI

Enregistrement des événements Insights pour un parcours à l'aide du AWS CLI

Pour vérifier si votre journal d'activité journalise les événements Insights, exécutez la commande `get-insight-selectors`.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

Le résultat suivant présente les paramètres par défaut pour un journal d'activité. Par défaut, les journaux d'activité ne journalisent pas les événements Insights. La valeur d'attribut `InsightType` est vide et aucun sélecteur d'événement Insight n'est spécifié, car la collecte des événements Insights n'est pas activée.

Si vous n'ajoutez pas de sélecteurs Insights, la get-insight-selectors commande renvoie le message d'erreur suivant : « Une erreur s'est produite (InsightNotEnabledException) lors de l'appel de l' GetInsightSelectors opération : Insights n'est pas activé sur le *nom du* sentier. Modifiez les paramètres du journal d'activité pour activer Insights, puis réessayez l'opération ».

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Pour configurer votre journal d'activité en sorte qu'il journalise les événements Insights, exécutez la commande `put-insight-selectors`. L'exemple suivant indique comment configurer votre journal d'activité pour inclure les événements Insights. Les valeurs du sélecteur Insights peuvent être `ApiCallRateInsight`, `ApiErrorRateInsight`, ou les deux.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Le résultat suivant montre le sélecteur d'événements Insights configuré pour le journal d'activité.

```
{
```

```
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Enregistrement des événements Insights pour une banque de données d'événements à l'aide du AWS CLI

Pour activer Insights sur un entrepôt de données d'événement, vous devez disposer d'un entrepôt de données d'événement source qui journalise les événements de gestion et d'un entrepôt de données d'événement de destination qui journalise les événements Insights.

Pour savoir si les événements Insights sont activés dans un entrepôt de données d'événement, exécutez la commande get-insight-selectors.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Pour savoir si un entrepôt de données d'événement est configuré pour recevoir des événements Insights ou des événements de gestion, exécutez la commande get-event-data-store.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

La procédure suivante vous explique comment créer les entrepôts de données d'événement de destination et de destination, puis activer les événements Insights.

1. Exécutez la commande aws cloudtrail create-event-data-store pour créer un entrepôt de données d'événement de destination qui collecte les événements Insights. La valeur pour `eventCategory` doit être `Insight`. Remplacez *`retention-period-days`*par le nombre de jours pendant lesquels vous souhaitez conserver les événements dans votre banque de données d'événements.

Si vous êtes connecté avec le compte de gestion d'une AWS Organizations organisation, incluez le `--organization-enabled` paramètre si vous souhaitez donner à votre administrateur délégué l'accès au magasin de données d'événements.

```
aws cloudtrail create-event-data-store \
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

Voici un exemple de réponse.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
```

```
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

Vous utiliserez l'ARN (ou le suffixe d'ID de l'ARN) de la réponse comme valeur du paramètre `--insights-destination` à l'étape 3.

2. Exécutez la commande aws cloudtrail create-event-data-store pour créer un entrepôt de données d'événement source qui journalise les événements de gestion. Par défaut, les entrepôts de données d'événement journalisent les événements de gestion et aucun événement de données. Il n'est pas nécessaire de spécifier les sélecteurs d'événements avancés si vous souhaitez journaliser tous les événements de gestion. Remplacez *retention-period-days*par le nombre de jours pendant lesquels vous souhaitez conserver les événements dans votre banque de données d'événements. Si vous créez un magasin de données d'événement d'organisation, incluez le paramètre `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

Voici un exemple de réponse.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
```

```
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Vous utiliserez l'ARN (ou le suffixe d'ID de l'ARN) de la réponse comme valeur du paramètre `--event-data-store` à l'étape 3.

3. Exécutez la commande put-insight-selectors pour activer les événements Insights. Les valeurs du sélecteur Insights peuvent être `ApiCallRateInsight`, `ApiErrorRateInsight`, ou les deux. Pour le paramètre `--event-data-store`, spécifiez l'ARN (ou le suffixe d'ID de l'ARN) de l'entrepôt de données d'événement source qui journalise les événements de gestion et activera Insights. Pour le paramètre `--insights-destination`, spécifiez l'ARN (ou le suffixe d'ID de l'ARN) de l'entrepôt de données d'événement de destination qui journalisera les événements Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Le résultat suivant montre le sélecteur d'événements Insights configuré pour l'entrepôt de données d'événement.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
```

```
        ]
}
```

Une fois que vous avez activé CloudTrail Insights pour la première fois dans un magasin de données d'événements, le lancement du premier événement Insights peut prendre jusqu' CloudTrail à 7 jours, si une activité inhabituelle est détectée.

CloudTrail Insights analyse les événements de gestion qui se produisent dans une seule région, et non à l'échelle mondiale. Un événement CloudTrail Insights est généré dans la même région que les événements de gestion connexes.

Dans le cas d'un magasin de données sur les événements d'une organisation, il CloudTrail analyse les événements de gestion du compte de chaque membre au lieu d'analyser l'agrégation de tous les événements de gestion de l'organisation.

Des frais supplémentaires s'appliquent pour l'ingestion d'événements Insights à CloudTrail Lake. Vous serez facturé séparément si vous activez Insights à la fois pour les journaux de suivi et les entrepôts de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Journalisation des événements avec les AWS SDK

Exécutez l'GetInsightSelectorsopération pour voir si votre banque de données de parcours ou d'événements active les événements Insights. Vous pouvez configurer vos parcours ou vos magasins de données d'événements pour activer les événements Insights avec l'PutInsightSelectorsopération. Pour plus d'informations, consultez la page Référence de l'API AWS CloudTrail.

Informations supplémentaires pour les journaux de suivi

Cette section fournit des informations supplémentaires spécifiques aux journaux de suivi. Cette section décrit comment vous pouvez consulter les événements relatifs aux parcours auxquels vous êtes abonné depuis la page Insights de la CloudTrail console et comment vous pouvez éventuellement envoyer ces événements à CloudWatch Logs à des fins de surveillance.

Rubriques

- Afficher les événements Insights pour les journaux de suivi dans la console
- Envoi d'événements de suivi à Amazon CloudWatch Logs

Afficher les événements Insights pour les journaux de suivi dans la console

Pour les pistes, vous pouvez également accéder aux événements Insights et les consulter sur la page Insights de la CloudTrail console. Pour plus d'informations sur la façon d'accéder aux événements Insights et de les afficher dans la console et à l'aide du AWS CLI, consultez Affichage CloudTrail des événements Insights pour les sentiers ce guide.

L'image suivante présente un exemple des événements Insights pour un journal de suivi. Vous ouvrez les pages de détails d'un événement Insights en choisissant un nom d'événement Insights dans les pages Dashboard (Tableau de bord) ou Insights.

Si vous désactivez CloudTrail Insights sur un trail ou si vous arrêtez de vous connecter à un trail (ce qui désactive CloudTrail Insights), il se peut que des événements Insights soient stockés dans votre compartiment S3 de destination, ou affichés sur la page Insights de la console, qui datent de la première fois que vous avez activé Insights.

Colonne Filtre

La colonne de gauche répertorie les événements Insights qui sont liés à l'API concerné, et qui ont le même type d'événement Insights. La colonne vous permet de choisir l'événement Insights sur lequel vous souhaitez obtenir plus d'informations. Lorsque vous choisissez un événement dans cette colonne, l'événement est mis en surbrillance dans le graphique de l'onglet Insights graph (Graphique Insights). Par défaut, CloudTrail applique un filtre qui limite les événements affichés dans l'onglet CloudTrailÉvénements à ceux relatifs à l'API spécifique qui a été appelée pendant la période d'activité inhabituelle qui a déclenché l'événement Insights. Pour afficher tous les CloudTrail événements appelés pendant la période d'activité inhabituelle, y compris les événements non liés à l'événement Insights, désactivez le filtre.

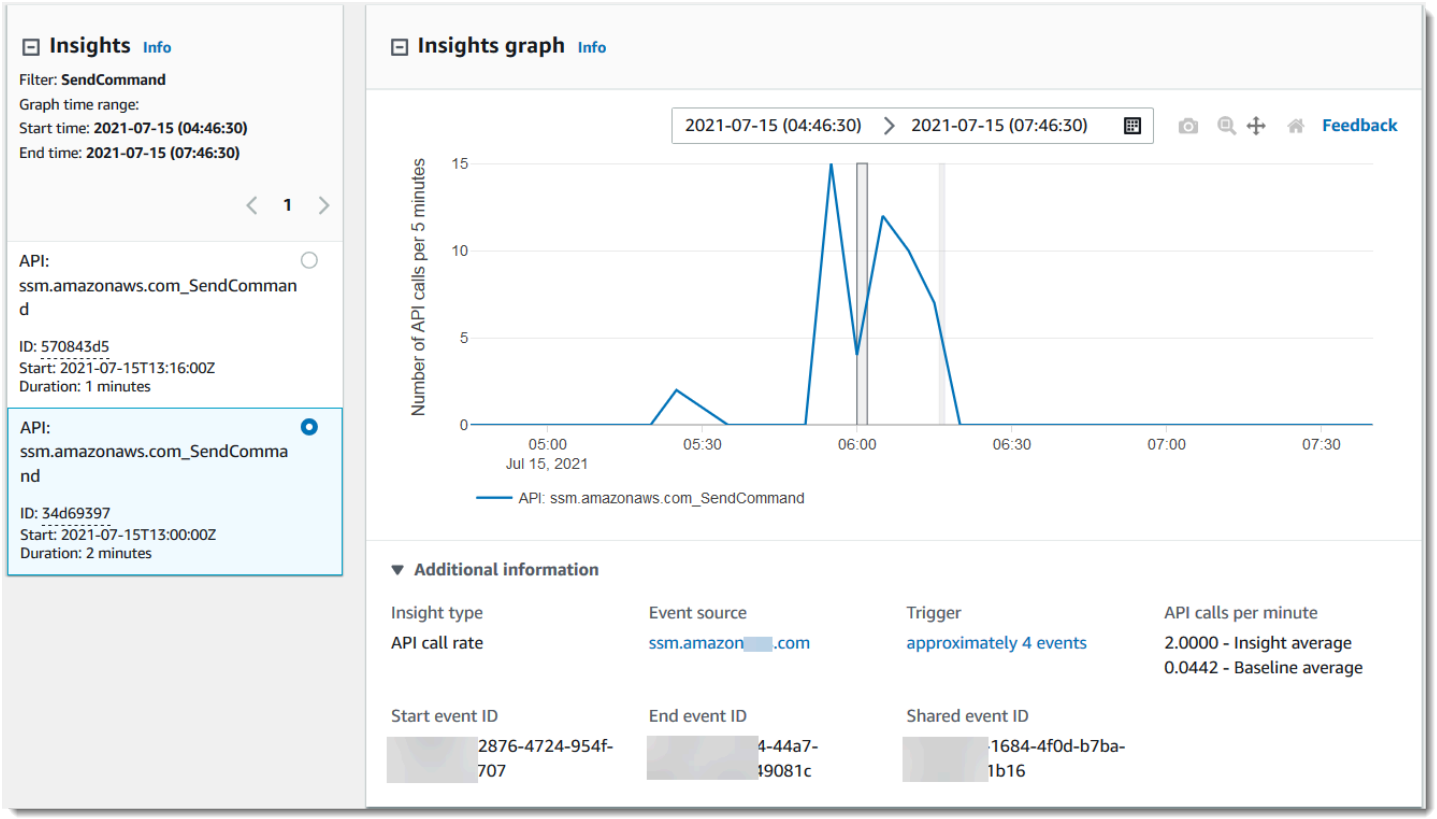
Onglet Graphique Insights

Dans l'onglet Insights graph (Graphique Insights), la page de détails d'un événement Insights présente un graphique du volume d'appel d'API ou un taux d'erreur d'une API ayant eu lieu avant et après qu'un ou plusieurs événements Insights aient été journalisés. Dans le graphique, les événements Insights sont mis en surbrillance avec des barres verticales, la largeur de la barre indiquant l'heure de début et de fin de l'événement Insights.

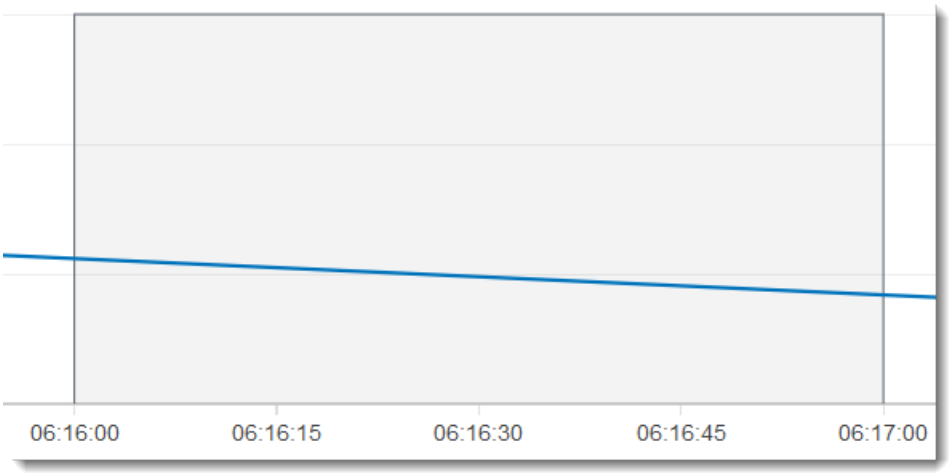
Dans cet exemple, une bande de surlignage verticale indique un nombre inhabituel d'appels d' AWS Systems Manager `SendCommand`API dans un compte. Dans la zone surlignée, le nombre d'`SendCommand`appels ayant dépassé la moyenne de référence du compte de 0,0442 appels par

minute, un événement Insights a été CloudTrail enregistré lorsqu'une activité inhabituelle a été détectée. L'événement Insights a enregistré que pas moins de 15 appels `SendCommand` ont été effectués pendant une période de cinq minutes entre 5 h 50 et 5 h 55. Il s'agit d'environ deux fois plus d'appels à cette API en plus par minute que prévu pour le compte. Dans cet exemple, la durée du graphique est de trois heures : de 4 h 30, le 15 juillet 2021 à 7 h 30 (heure d'été du Pacifique), le 15 juillet 2021 (heure d'été du Pacifique). Cet événement commence à 06 h 00, le 15 juillet 2021 (heure d'été du Pacifique) et une heure de fin deux minutes plus tard. Un événement de fin Insights, non mis en surbrillance, montre que l'activité inhabituelle s'est terminée vers 6 h 16.

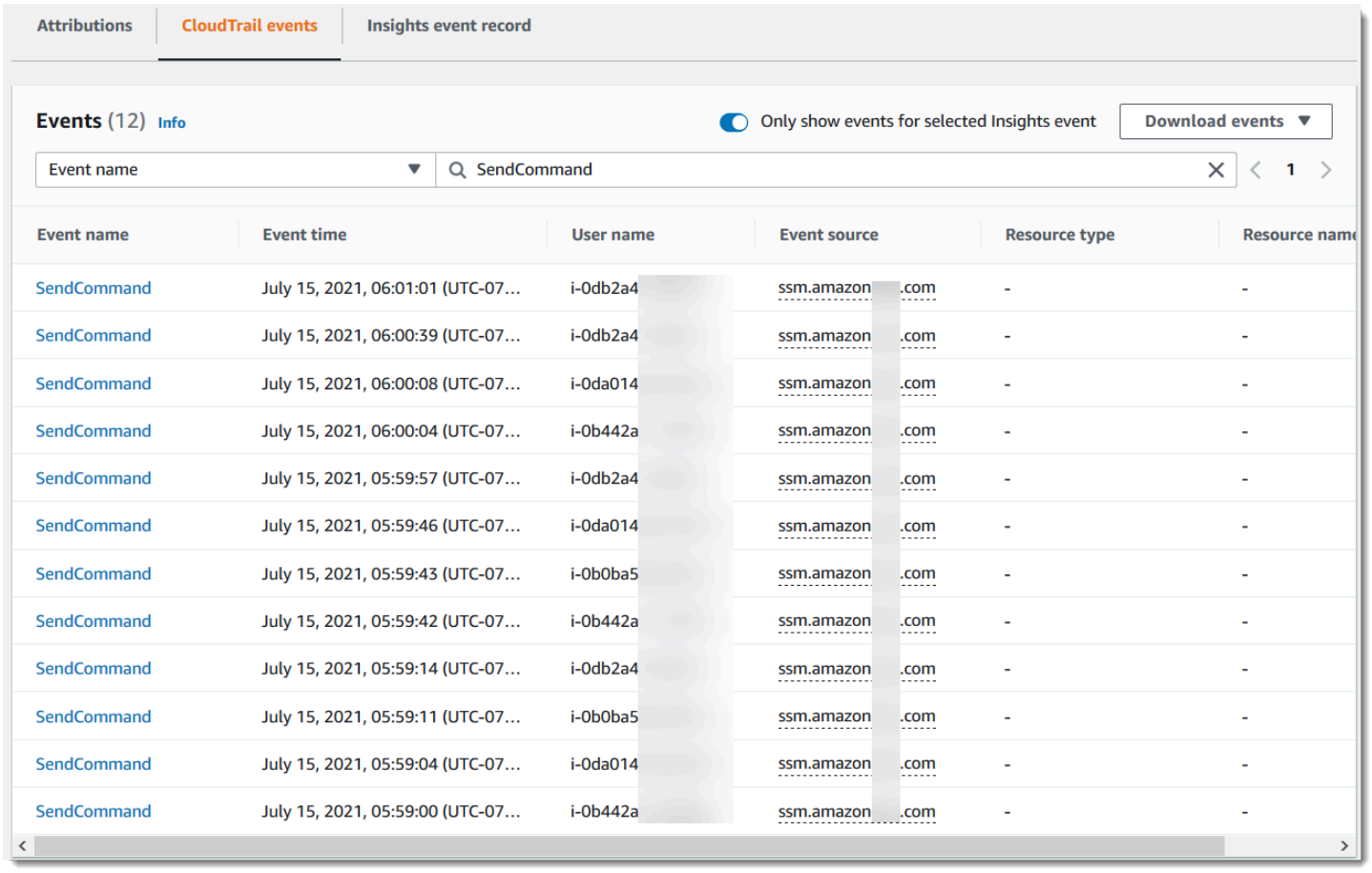
La référence est calculée sur les sept jours précédant le début d'un événement Insights. Bien que la valeur de la durée de référence, c'est-à-dire la période d' CloudTrail analyse de l'activité normale sur les API, soit d'environ sept jours, CloudTrail arrondie la durée de référence à un jour entier, de sorte que la durée de référence exacte peut varier.



Vous pouvez utiliser le plugin Zoom sur la barre d'outils pour zoomer sur l'événement Insights de fin, indiquant les heures de début et de fin. Dans cet exemple, en choisissant Zoom, puis en faisant glisser le curseur Zoom sur une très courte distance sur un bord de l'événement Insights mis en surbrillance, vous élargissez l'événement Insights et affichez plus de détails sur la chronologie.

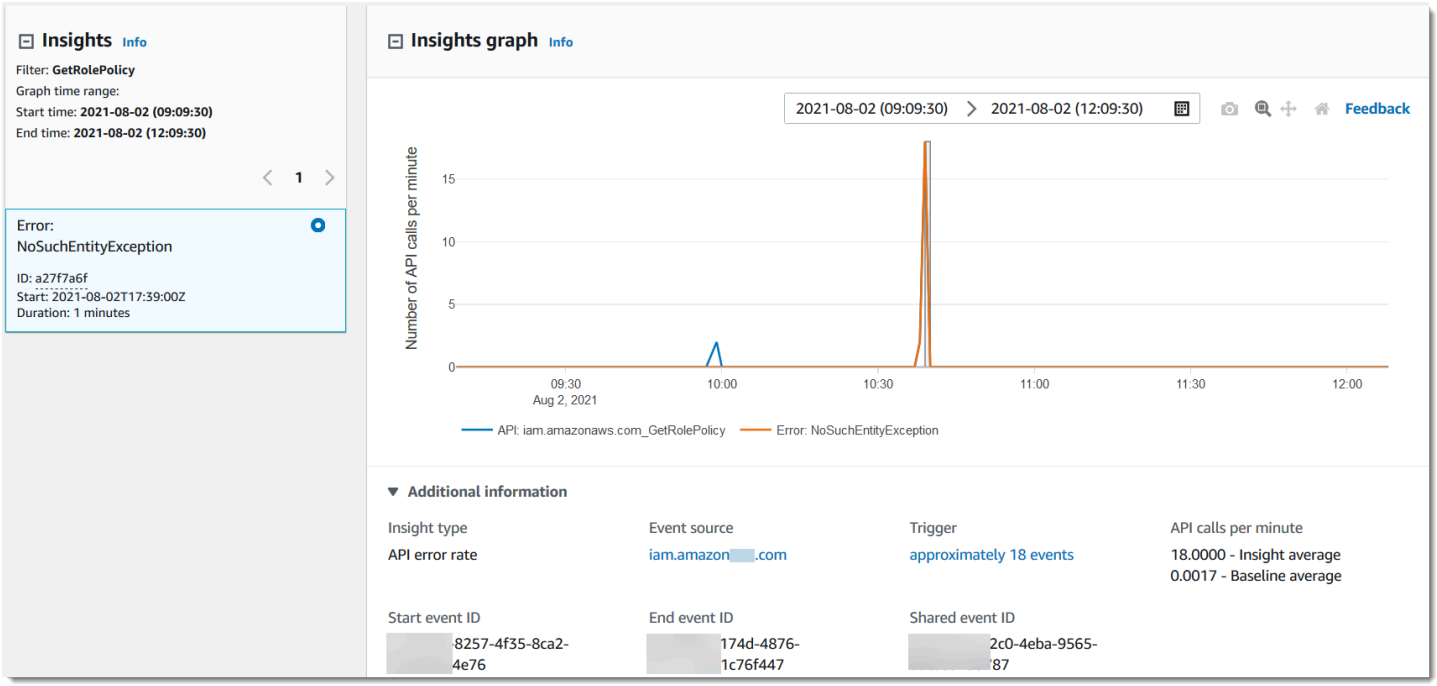


Pour afficher CloudTrail les événements analysés afin de déterminer une activité inhabituelle, ouvrez l'onglet CloudTrail Événements. Dans cet exemple, 12 événements CloudTrail ont été analysés, dont quatre ont déclenché l'événement Insights.



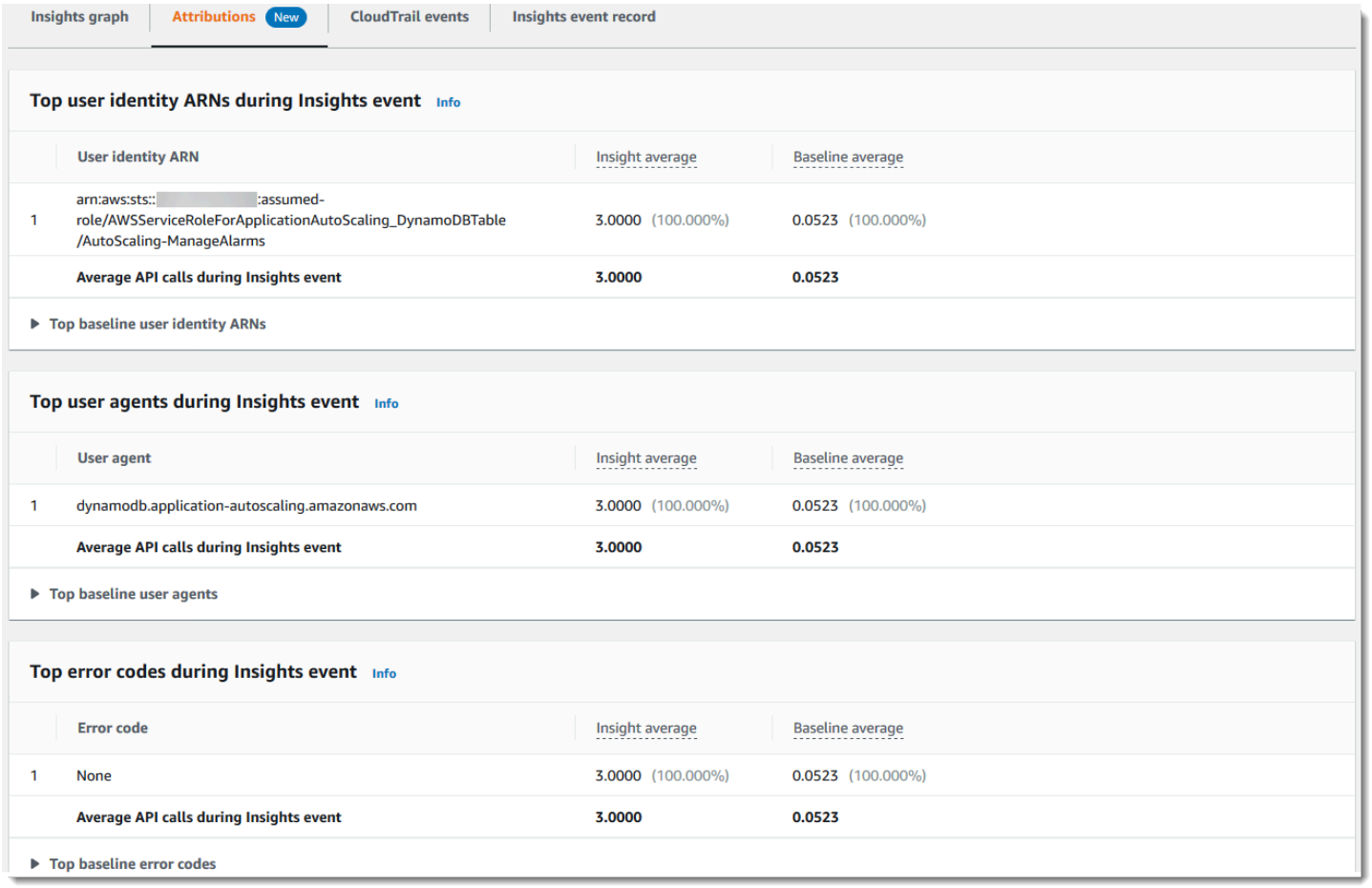
La capture d'écran suivante présente un onglet de graphique Insights pour un événement Insights de taux d'erreur de l'API. La zone mise en surbrillance indique qu'un événement Insights a été journalisé

car les occurrences de l' `NoSuchEntityException` erreur sur l' `GetRolePolicy` appel d'API IAM ont augmenté au-dessus de la moyenne de référence de 0,0017 `NoSuchEntityException` erreurs par minute lors de cet appel d'API, soit une moyenne de 18 erreurs par minute pendant la période d'information. Le nombre d' CloudTrail événements qui ont déclenché l'événement Insights correspond à la moyenne de 18 `NoSuchEntityException` erreurs d'Insights en une minute, dans cet exemple. Contrairement à un graphique de taux d'appels d'API, le taux d'erreur de l'API affiche deux lignes, dans des couleurs contrastées : une ligne mesurant les appels à l'API IAM, `GetRolePolicy`, qui a entraîné un nombre inhabituel d'erreurs et une ligne mesurant l'erreur sur laquelle une activité inhabituelle a été journalisée `NoSuchEntityException`.

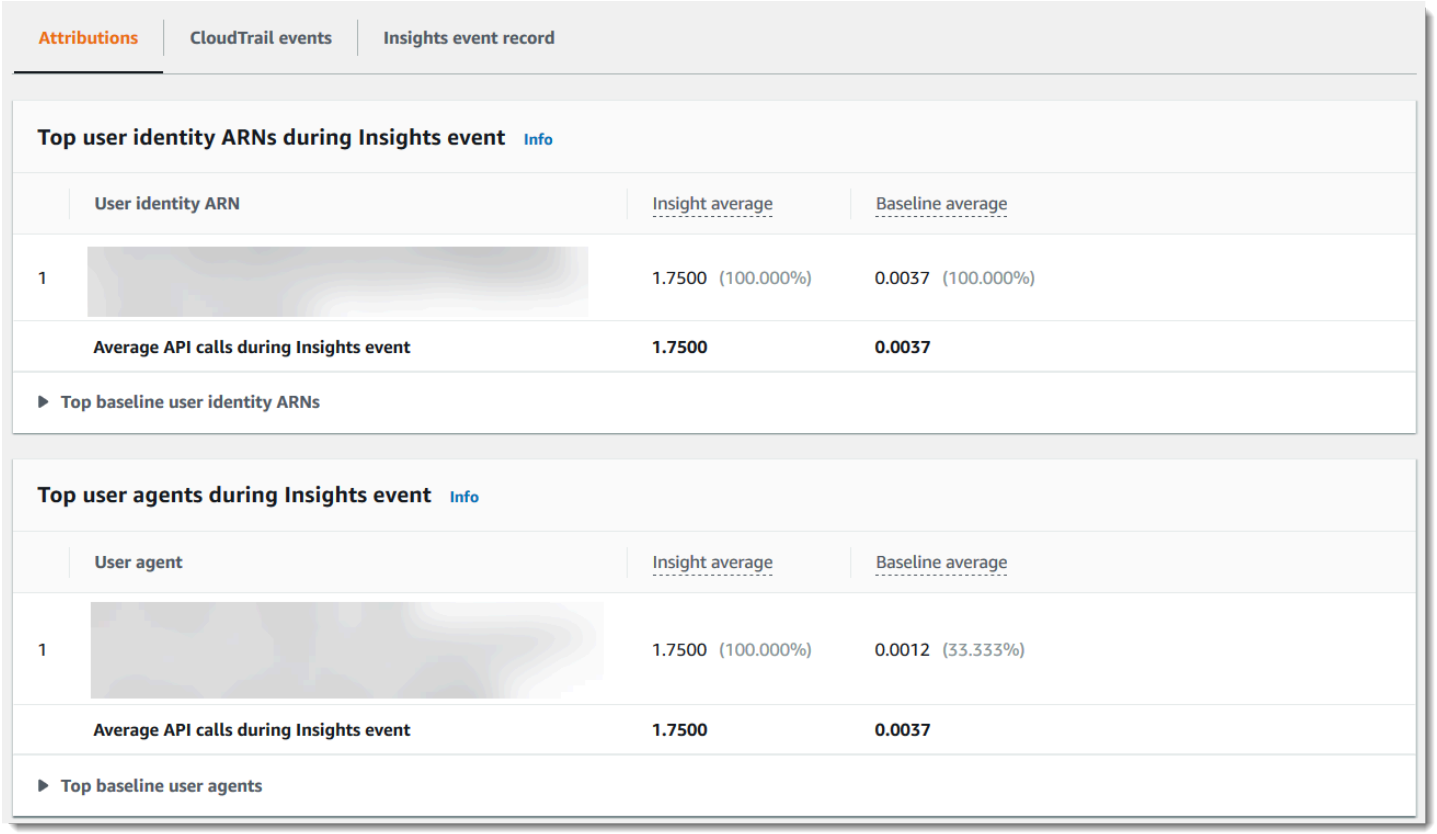


Onglet Attributions

L'onglet Attributions affiche les informations suivantes relatives à un événement Insights. L'information sur l'onglet Attributions peut vous aider à identifier les causes et les sources de l'activité Insights. Développez les principales zones de référence pour comparer l'identité utilisateur, l'agent utilisateur et l'activité du code d'erreur pendant les périodes normales avec celles attribuées pendant l'activité Insights. Dans Principaux ARN d'identité utilisateur de référence, Principaux agents utilisateurs de référence et Principaux codes d'erreur de référence, uniquement la moyenne de référence (la moyenne historique des événements de l'API qui sont journalisés par l'identité utilisateur, l'agent utilisateur ou qui entraînent le code d'erreur, environ sept jours avant l'heure de début de l'événement Insights) est affichée.



L'onglet Attributions affiche uniquement les principaux ARN d'identité utilisateur et les principaux agents utilisateur pour un événement Insights de taux d'erreur, comme illustré dans l'image suivante. Les principaux codes d'erreur ne sont pas nécessaires pour les événements Insights de taux d'erreur.



- Principaux ARN d'identité utilisateur - Ce tableau présente les cinq principaux AWS utilisateurs ou rôles IAM (identités utilisateur) ayant contribué aux appels d'API pendant les périodes d'activité et de référence inhabituelles, par ordre décroissant selon le nombre moyen d'appels d'API fournis. Le pourcentage des moyennes en tant que total de l'activité ayant contribué à l'activité inhabituelle est indiqué entre parenthèses. Si plus de cinq ARN d'identité utilisateur ont contribué à l'activité inhabituelle, leur activité sera résumée dans une autre ligne.
- Principaux agents utilisateurs - Ce tableau présente les cinq principaux AWS outils par lesquels l'identité de l'utilisateur a contribué aux appels d'API au cours de l'activité inhabituelle et des périodes de référence, par ordre décroissant du nombre moyen d'appels d'API fournis. Ces outils incluent le AWS Management Console AWS CLI, ou les AWS SDK. Par exemple, un agent utilisateur nommé `ec2.amazonaws.com` indique que la console Amazon EC2 faisait partie des outils utilisés pour appeler l'API. Le pourcentage des moyennes en tant que total de l'activité ayant contribué à l'activité inhabituelle est indiqué entre parenthèses. Si plus de cinq agents utilisateur ont contribué à l'activité inhabituelle, leur activité sera résumée dans une autre ligne.
- Principaux codes d'erreur - Affichés uniquement pour les événements Insights de taux d'appel d'API. Ce tableau indique les cinq principaux codes d'erreur qui se sont produits sur les appels d'API pendant les périodes d'activité inhabituelles et de référence, dans l'ordre décroissant du

plus grand nombre d'appels d'API au plus petit. Le pourcentage des moyennes en tant que total de l'activité ayant contribué à l'activité inhabituelle est indiqué entre parenthèses. Si plus de cinq codes d'erreur se sont produits au cours de l'activité inhabituelle ou de référence, leur activité sera résumée dans une autre ligne.

Une valeur de None comme l'une des cinq principales valeurs de code d'erreur signifie qu'un pourcentage significatif des appels ayant contribué à l'événement Insights n'a pas entraîné d'erreurs. Si la valeur du code d'erreur estNone, et il n'y a pas d'autres codes d'erreur dans la table, les valeurs des colonnes Insights average (Moyenne Insights) et Baseline average (Moyenne de référence) sont identiques à celles de l'événement Insights globalement. Vous pouvez également afficher ces valeurs dans la fenêtre Insight average (Moyenne Insight) et Baseline average (Moyenne de référence) sous l'onglet Insights graph (Graphique Insights), sous Appels d'API par minute.

Moyenne de référence et moyenne Insights

Moyenne de référence et Moyenne Insights sont affichés pour les principales identités d'utilisateur, les principaux agents utilisateur et les principaux codes d'erreur.

- Baseline average (Moyenne de référence) : taux standard d'appels par minute vers cette API sur lequel l'évènement Insights a été journalisé, mesuré au cours de la semaine précédente, dans une région spécifique de votre compte.
- Insights average (Moyenne Insights) : taux d'appels par minute ou d'erreur à cette API ayant déclenché l'événement Insights. La moyenne d' CloudTrail Insights pour l'événement de démarrage est le taux d'appels ou d'erreurs par minute sur l'API qui a déclenché l'événement Insights. Généralement, il s'agit de la première minute d'activité inhabituelle. La moyenne Insights pour l'événement de fin est le taux d'appels d'API ou d'erreurs par minute pendant la durée de l'activité inhabituelle, entre l'événement Insights de démarrage et l'événement Insights de fin.

CloudTrail onglet événements

Dans l'onglet CloudTrail Événements, consultez les événements connexes CloudTrail analysés pour déterminer qu'une activité inhabituelle s'est produite. Par défaut, un filtre est déjà appliqué pour le nom de l'événement Insights, qui est également le nom de l'API associée. Pour afficher tous les CloudTrail événements enregistrés pendant la période d'activité inhabituelle, désactivez Afficher uniquement les événements pour l'événement Insights sélectionné. L'onglet CloudTrail événements affiche les événements de CloudTrail gestion liés à l'API en question survenus entre le début et la fin

de l'événement Insights. Ces événements vous aident à effectuer une analyse plus approfondie afin de déterminer la cause probable d'un événement Insights et les raisons de l'activité inhabituelle de l'API et l'activité de taux d'erreur.

Onglet Insights event record (Enregistrement des événements Insights)

Comme tout CloudTrail événement, un événement CloudTrail Insights est un enregistrement au format JSON. L'onglet Insights event record (Enregistrement des événements Insights) affiche la structure JSON et le contenu des événements de début et de fin Insights, parfois appelés (charge utile) de l'événement. Pour plus d'informations sur les champs et le contenu de l'enregistrement de l'événement Insights, consultez Champs d'enregistrement pour les événements Insights et CloudTrail `insightDetails`Élément Insights dans ce guide.

Envoi d'événements de suivi à Amazon CloudWatch Logs

CloudTrail prend en charge l'envoi d'événements Insights pour les sentiers à CloudWatch Logs. Lorsque vous configurez votre suivi pour envoyer des événements Insights à votre groupe de CloudWatch journaux Logs, CloudTrail Insights envoie uniquement les événements que vous spécifiez dans votre journal. Par exemple, si vous configurez votre suivi pour enregistrer les événements de gestion et d'Insights, il fournit des événements de gestion et d'Insights à votre groupe de CloudWatch journaux Logs. Pour plus d'informations, voir Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.

CloudTrail enregistrer le contenu

Le corps de l'enregistrement contient les champs qui permettent de déterminer l'action demandée, ainsi que le moment et l'endroit où la demande a été effectuée. Lorsque la valeur d'Optional (Facultatif) est True (Vraie), le champ est uniquement présent lorsqu'il s'applique au service, à l'API ou au type d'événement. Une valeur Optional (Facultatif) de False (Faux) signifie que le champ est soit toujours présent ou que sa présence ne dépend pas du service, de l'API ou du type d'événement. Voici un exemple : `responseElements`, qui est présent dans les événements pour les actions qui apportent des modifications (actions de création, de mise à jour ou de suppression).

CloudTrail tronque un champ si son contenu dépasse la taille maximale du champ. Si un champ est tronqué, `omitted` est présent avec une valeur de `true`.

`eventTime`

Date et heure de la demande, en heure UTC (temps universel coordonné). L'horodatage d'un événement provient de l'hôte local qui fournit le point de terminaison de l'API de service sur lequel

l'appel d'API a été effectué. Par exemple, un événement d'CreateBucketAPI exécuté dans la région de l'ouest des États-Unis (Oregon) sera horodaté à partir de l'heure sur un AWS hôte exécutant le point de terminaison Amazon S3,`s3.us-west-2.amazonaws.com`. En général, les AWS services utilisent le protocole NTP (Network Time Protocol) pour synchroniser les horloges de leur système.

Depuis : 1.0

Facultatif : False

`eventVersion`

Version du format de l'événement du journal. La version actuelle est la 1.10.

La valeur `eventVersion` est une version majeure et une version mineure au format *`major_version`*.*`minor_version`*. Par exemple, vous pouvez disposer d'une valeur `eventVersion` de `1.09`, où `1` représente la version majeure, et `09`, la version mineure.

CloudTrail incrémente la version principale si une modification non rétrocompatible est apportée à la structure de l'événement. Cela inclut la suppression d'un champ JSON qui existe déjà ou la modification de la façon dont le contenu d'un champ est représenté (par exemple, un format de date). CloudTrail augmente la version mineure si une modification ajoute de nouveaux champs à la structure de l'événement. Cela peut se produire si de nouvelles informations sont disponibles pour tout ou partie des événements existants, ou si de nouvelles informations sont disponibles seulement pour des types d'événements nouvellement introduits. Les applications peuvent ignorer les nouveaux champs pour être compatibles avec de nouvelles versions mineures de la structure de l'événement.

Si de CloudTrail nouveaux types d'événements sont introduits, mais que la structure de l'événement reste inchangée, la version de l'événement ne change pas.

Pour vous assurer que vos applications puissent analyser la structure de l'événement, nous vous recommandons d'effectuer une comparaison égal à sur le numéro de version majeure. Pour être sûr que les champs attendus par votre application existent, nous vous recommandons également d'effectuer une comparaison greater-than-or-equal -to sur la version mineure. La version mineure ne comporte pas de zéros au début. Vous pouvez interpréter à la fois *`major_version`* et *`minor_version`* en tant que nombres, et effectuer des opérations de comparaison.

Depuis : 1.0

Facultatif : False

`userIdentity`

Informations sur l'identité IAM qui a émis une demande. Pour plus d'informations, consultez CloudTrail Élément UserIdentity.

Depuis : 1.0

Facultatif : False

`eventSource`

Service auprès duquel la demande a été faite. Ce nom est généralement une forme abrégée du nom du service sans espaces, plus `.amazonaws.com`. Par exemple :

- AWS CloudFormation est`cloudformation.amazonaws.com`.
- Amazon EC2 est `ec2.amazonaws.com`.
- Amazon Simple Workflow Service est `swf.amazonaws.com`.

Cette convention présente quelques exceptions. Par exemple, `eventSource` pour Amazon, CloudWatch c'est`monitoring.amazonaws.com`.

Depuis : 1.0

Facultatif : False

`eventName`

Action demandée, qui est l'une des actions de l'API pour ce service.

Depuis : 1.0

Facultatif : False

`awsRegion`

Le Région AWS destinataire de la demande, tel que`us-east-2`. Consultez CloudTrail Régions prises en charge.

Depuis : 1.0

Facultatif : False

`sourceIPAddress`

Adresse IP à partir de laquelle la demande a été faite. Pour les actions qui sont créées à partir de la console de service, l'adresse présentée est celle de la ressource du client sous-jacent, non le serveur Web de la console. Pour les services en AWS entrée, seul le nom DNS est affiché.

> **Note**
>
> Pour les événements émis par AWS, ce champ est généralement `AWS Internal/#`, où `#` est un nombre utilisé à des fins internes.

Depuis : 1.0

Facultatif : False

`userAgent`

L'agent via lequel la demande a été effectuée, tel que le AWS Management Console, un AWS service, les AWS SDK ou le AWS CLI. Ce champ a une taille maximale de 1 Ko ; tout contenu dépassant cette limite est tronqué. Voici quelques exemples de valeurs :

- `lambda.amazonaws.com` – La demande a été effectuée avec AWS Lambda.
- `aws-sdk-java` – La demande a été effectuée avec le AWS SDK for Java.
- `aws-sdk-ruby` – La demande a été effectuée avec le AWS SDK for Ruby.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— La demande a été faite avec le système AWS CLI installé sur Linux.

> **Note**
>
> Pour les événements créés par AWS, si CloudTrail vous savez qui Service AWS a effectué l'appel, ce champ est la source de l'événement du service d'appel (par exemple,`ec2.amazonaws.com`). Dans le cas contraire, ce champ est`AWS Internal/#`, où `#` est un numéro utilisé à des fins internes.

Depuis : 1.0

Facultatif : True

`errorCode`

Erreur de AWS service si la demande renvoie une erreur. Pour obtenir un exemple qui montre ce champ, consultez Exemple de code d'erreur et de journal de messages. Ce champ a une taille maximale de 1 Ko ; tout contenu dépassant cette limite est tronqué.

Depuis : 1.0

Facultatif : True

`errorMessage`

Si la demande renvoie une erreur, description de l'erreur. Ce message inclut des messages relatifs à des échecs d'autorisation. CloudTrail capture le message enregistré par le service dans sa gestion des exceptions. Pour voir un exemple, consultez Exemple de code d'erreur et de journal de messages. Ce champ a une taille maximale de 1 Ko ; tout contenu dépassant cette limite est tronqué.

> **Note**
>
> Certains AWS services fournissent les champs `errorCode` et `errorMessage` en tant que champs de haut niveau lors de l'événement. D'autres services AWS fournissent des informations d'erreur dans le cadre de `responseElements`.

Depuis : 1.0

Facultatif : True

`requestParameters`

Les paramètres, le cas échéant, qui ont été envoyées avec la demande. Ces paramètres sont documentés dans la documentation de référence de l'API pour le AWS service approprié. Ce champ a une taille maximale de 100 Ko ; tout contenu dépassant cette limite est tronqué.

Depuis : 1.0

Facultatif : False

`responseElements`

Les éléments de réponse, le cas échéant, pour les actions apportant des modifications (actions de création, de mise à jour ou de suppression). Si l'action ne renvoie pas d'éléments de réponse, ce champ l'est`null`. Si une action ne change pas d'état (par exemple, une demande pour obtenir ou répertorier des objets), cet élément est omis. Les éléments de réponse aux actions sont documentés dans la référence de l'API documentation pour le produit approprié Service AWS. Ce champ a une taille maximale de 100 Ko ; le contenu dépassant cette limite est tronqué.

La `responseElements` valeur est utile pour vous aider à suivre une demande avec AWS Support. Les deux `x-amz-request-id` et `x-amz-id-2` contiennent des informations qui vous aident à suivre une demande auprès de AWS Support. Ces valeurs sont les mêmes que ceux que le service renvoie en réponse à la demande initie les événements, afin que vous puissiez les utiliser pour faire correspondre l'événement à demande.

Depuis : 1.0

Facultatif : False

`additionalEventData`

Des données supplémentaires sur l'événement qui ne faisaient pas partie de la demande ou de la réponse. Ce champ a une taille maximale de 28 Ko ; tout contenu dépassant cette limite est tronqué.

Depuis : 1.0

Facultatif : True

`requestID`

Valeur qui identifie la demande. Le service appelé génère cette valeur. Ce champ a une taille maximale de 1 Ko ; tout contenu dépassant cette limite est tronqué.

Depuis : 1.01

Facultatif : True

`eventID`

GUID généré par CloudTrail pour identifier de manière unique chaque événement. Vous pouvez utiliser cette valeur pour identifier un événement unique. Par exemple, vous pouvez utiliser l'ID comme clé primaire pour récupérer les données des journaux à partir d'une base de données dans laquelle vous pouvez effectuer des recherches.

Depuis : 1.01

Facultatif : False

`eventType`

Identifie le type d'événement qui a généré l'enregistrement de l'événement. Il peut s'agir de l'une des valeurs suivantes :

- `AwsApiCall` – Une API a été appelée.
- `AwsServiceEvent` – Le service a généré un événement lié à votre journal d'activité. Par exemple, cela peut se produire lorsqu'un autre compte a effectué un appel avec une ressource dont vous êtes propriétaire.
- `AwsConsoleAction` – Une action a été effectuée dans la console et qui n'était pas un appel d'API.
- `AwsConsoleSignIn`— Un utilisateur de votre compte (root, IAM, fédéré, SAML ou SwitchRole) s'est connecté au. AWS Management Console
- `AwsCloudTrailInsight`— Si les événements Insights sont activés, CloudTrail génère des événements Insights lorsqu'une activité opérationnelle inhabituelle est CloudTrail détectée, telle que des pics dans le provisionnement des ressources ou des rafales d'actions AWS Identity and Access Management (IAM).

  Les événements `AwsCloudTrailInsight` n'utilisent pas les champs suivants :

  - `eventName`
  - `eventSource`
  - `sourceIPAddress`
  - `userAgent`
  - `userIdentity`

Depuis : 1.02

Facultatif : False

`apiVersion`

Identifie la version de l'API associée à la valeur `AwsApiCall` `eventType`.

Depuis : 1.01

Facultatif : True

`managementEvent`

Valeur booléenne qui identifie si l'événement est un événement de gestion. `managementEvent` s'affiche dans un enregistrement d'événement si `eventVersion` est la version 1.06 ou supérieure et que le type d'événement est l'un des types suivants :

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

Depuis : 1.06

Facultatif : True

`readOnly`

Identifie si cette opération est en lecture seule. Il peut s'agir de l'une des valeurs suivantes :

- `true` – L'opération est en lecture seule (par exemple, `DescribeTrails`).
- `false` – L'opération est en écriture seule (par exemple, `DeleteTrail`).

Depuis : 1.01

Facultatif : True

`resources`

Une liste des ressources consultées dans l'événement. Le champ peut contenir les informations suivantes :

- ARN de la ressource
- ID de compte du propriétaire de la ressource
- Identifiant du type de ressource au format : `AWS::aws-service-name::data-type-name`

Par exemple, quand un événement `AssumeRole` est consigné, le champ `resources` peut apparaître comme ce qui suit :

- ARN : `arn:aws:iam::123456789012:role/myRole`
- ID de compte : `123456789012`
- Identifiant du type de ressource : `AWS::IAM::Role`

Par exemple, les journaux contenant le `resources` champ sont répertoriés dans la section Événement d'AWS STS API dans le fichier CloudTrail journal du guide de l'utilisateur IAM ou journalisation des appels d' AWS KMS API dans le guide du AWS Key Management Service développeur.

Depuis : 1.01

Facultatif : True

`recipientAccountId`

Représente l'ID du compte qui a reçu cet événement. L'élément `recipientAccountID` peut être différent de CloudTrail Élément UserIdentity `accountId`. Cela peut se produire dans l'accès aux ressources entre comptes. Par exemple, si une clé CMK, également appelée AWS KMS key, a été utilisée par un compte distinct pour appeler l'API de chiffrement, les valeurs `accountId` et `recipientAccountID` sont les mêmes pour l'événement livré au compte qui a effectué l'appel, mais elles sont différentes pour l'événement qui est livré au compte qui possède la clé CMK.

Depuis : 1.02

Facultatif : True

`serviceEventDetails`

Identifie l'événement de service, y compris ce qui le déclenche et le résultat. Pour plus d'informations, consultez AWS événements de service. Ce champ a une taille maximale de 100 Ko ; tout contenu dépassant cette limite est tronqué.

Depuis : 1.05

Facultatif : True

`sharedEventID`

GUID généré par CloudTrail pour identifier de manière unique les CloudTrail événements AWS d'une même action envoyée à différents AWS comptes.

Par exemple, lorsqu'un compte utilise un AWS KMS keycompte appartenant à un autre compte, le compte qui a utilisé la clé KMS et le compte propriétaire de la clé KMS reçoivent des CloudTrail événements distincts pour la même action. Chaque CloudTrail événement organisé pour cette AWS action partage la même chose`sharedEventID`, mais possède également un `eventID` et unique`recipientAccountID`.

Pour plus d'informations, consultez Exemple de sharedEventID.

> **Note**
>
> Le `sharedEventID` champ n'est présent que lorsque les CloudTrail événements sont transmis à plusieurs comptes. Si l'appelant et le propriétaire sont le même AWS compte, CloudTrail envoie un seul événement et le `sharedEventID` champ n'est pas présent.

Depuis : 1.03

Facultatif : True

`vpcEndpointId`

Identifie le point de terminaison VPC dans lequel les demandes ont été effectuées d'un VPC vers un autre service AWS , comme Amazon S3.

Depuis : 1.04

Facultatif : True

`eventCategory`

Affiche la catégorie de l'événement. Le `eventCategory` est utilisé dans les `LookupEvents`appels à la direction et les événements Insights.

- Pour les événements de gestion, la valeur est `Management`.
- Pour les événements de données, la valeur est `Data`.
- Pour les événements Insights, la valeur est `Insight`.

Depuis : 1.07

Facultatif : False

`addendum`

Si la livraison d'un événement a été retardée ou si des informations supplémentaires sur un événement existant sont disponibles après l'enregistrement de l'événement, un champ addenda affiche des informations sur les raisons pour lesquelles l'événement a été retardé. Si des informations manquaient dans un événement existant, le champ addenda inclut les informations manquantes et une raison pour laquelle elles étaient manquantes. Le contenu comprend les éléments suivants :

- **`reason`** - La raison pour laquelle l'événement ou une partie de son contenu était manquant. Il peut s'agir de l'une des valeurs suivantes :
  - **`DELIVERY_DELAY`** – Il y a eu un retard de livraison des événements. Cela peut être dû à un trafic réseau élevé, à des problèmes de connectivité ou à un problème CloudTrail de service.
  - **`UPDATED_DATA`** – Un champ de l'enregistrement d'événement manquait ou comportait une valeur incorrecte.
  - **`SERVICE_OUTAGE`**— Un service qui enregistre les événements en CloudTrail cas de panne et qui n'a pas pu les enregistrer CloudTrail. Ceci est extrêmement rare.
- **`updatedFields`** - Les champs d'enregistrement d'événement mis à jour par l'addenda. Ceci n'est fourni que si la raison est `UPDATED_DATA`.
- **`originalRequestID`** - ID unique d'origine de la demande. Ceci n'est fourni que si la raison est `UPDATED_DATA`.
- **`originalEventID`** - ID d'événement d'origine. Ceci n'est fourni que si la raison est `UPDATED_DATA`.

Depuis : 1.08

Facultatif : True

`sessionCredentialFromConsole`

Indique si un événement est issu d'une AWS Management Console session. Ce champ n'est pas affiché sauf si la valeur est `true`, ce qui signifie que le client utilisé pour effectuer l'appel d'API

était soit un proxy, soit un client externe. Si un client proxy a été utilisé, le champ d'événement `tlsDetails` n'est pas affiché.

Depuis : 1.08

Facultatif : True

`edgeDeviceDetails`

Affiche des informations sur les périphériques cibles d'une demande. Actuellement, les événements du périphérique `S3 Outposts` incluent ce champ. Ce champ a une taille maximale de 28 Ko ; tout contenu dépassant cette limite est tronqué.

Depuis : 1.08

Facultatif : True

`tlsDetails`

Affiche des informations sur la version TLS (Transport Layer Security), les suites de chiffrement et le nom de domaine complet (FQDN) du nom d'hôte fourni par le client utilisé dans l'appel d'API de service, qui est généralement le nom de domaine complet du point de terminaison du service. CloudTrailenregistre toujours des informations TLS partielles si les informations attendues sont manquantes ou vides. Par exemple, si la version TLS et la suite de chiffrement sont présentes, mais que l'`HOST`en-tête est vide, les détails TLS disponibles sont toujours enregistrés dans l'événement. CloudTrail

- **`tlsVersion`** : La version TLS d'une demande.
- **`cipherSuite`** : La suite de chiffrement (combinaison d'algorithmes de sécurité utilisés) d'une requête.
- **`clientProvidedHostHeader`** : Le nom d'hôte fourni par le client utilisé dans l'appel d'API de service, qui est généralement le nom de domaine pleinement qualifié (FQDN) du point de terminaison du service.

> **Note**
>
> Dans certains cas, le champ `tlsDetails` n'est pas présent dans un enregistrement d'événement.
>
> - Le `tlsDetails` champ n'est pas présent si l'appel d'API a été effectué par un Service AWS utilisateur en votre nom. Le champ `invokedBy` de l'élément `userIdentity` identifie l' Service AWS qui a effectué l'appel d'API.

- Si `sessionCredentialFromConsole` est présent avec la valeur true, `tlsDetails` est présent dans un enregistrement d'événement uniquement si un client externe a été utilisé pour effectuer l'appel d'API.

Depuis : 1.08

Facultatif : True

Champs d'enregistrement pour les événements Insights

Les attributs suivants sont affichés dans la structure JSON d'un événement Insights et diffèrent de ceux d'un événement de gestion ou de données.

`sharedEventId`

Les événements A `sharedEventID` pour CloudTrail Insights sont différents des CloudTrail événements `sharedEventID` relatifs à la gestion et aux types de données. Dans les événements Insights, a `sharedEventID` est un GUID généré par CloudTrail Insights pour identifier de manière unique un événement Insights. `sharedEventID`Dest courant entre les événements Insights de début et de fin, et permet de relier les deux événements afin d'identifier de manière unique les activités inhabituelles. Vous pouvez considérer `sharedEventID` comme l'ID d'événement Insights global.

Depuis : 1.07

Facultatif : False

`insightDetails`

Événements Insights uniquement. Affiche des informations sur les déclencheurs sous-jacents d'un événement Insights, comme la source de l'événement, l'agent utilisateur, les statistiques, le nom de l'API. Il indique également si l'événement est le début ou la fin de l'événement Insights. Pour plus d'informations sur le contenu du bloc `insightDetails`, consultez CloudTrail `insightDetails`Élément Insights.

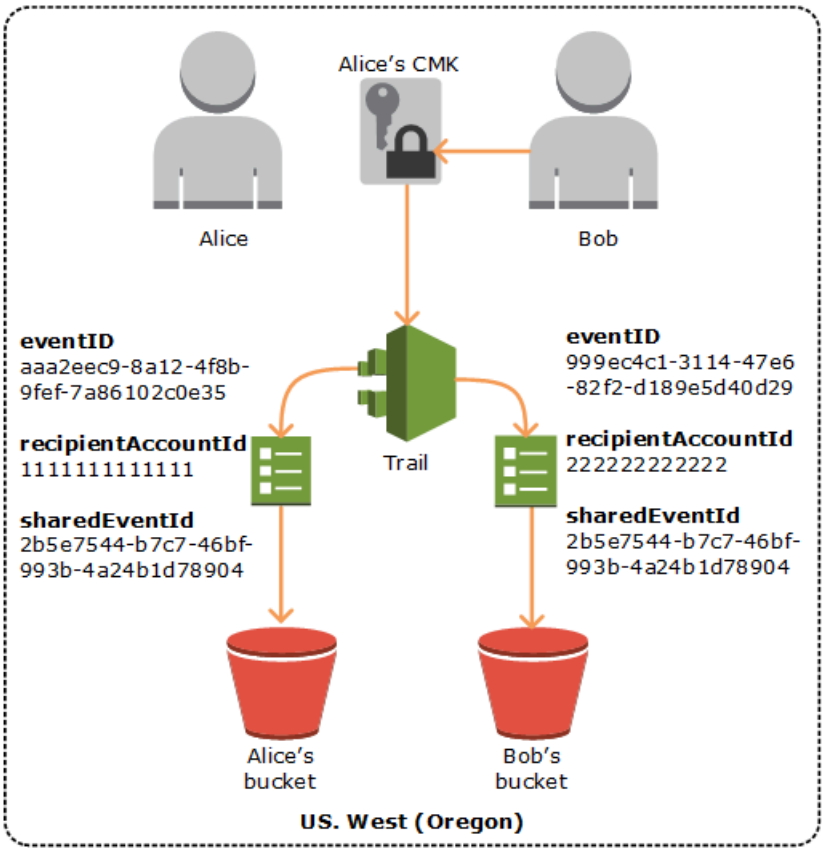
Depuis : 1.07

Facultatif : False

Exemple de sharedEventID

L'exemple suivant décrit comment CloudTrail délivre deux événements pour la même action :

1. Alice possède un AWS compte (111111111111) et crée un. AWS KMS key Elle est propriétaire de cette clé KMS.
2. Bob a un AWS compte (222222222222). Alice donne à Bob l'autorisation d'utiliser la clé KMS.
3. Chaque compte a un journal de suivi et un compartiment distinct.
4. Bob utilise la clé KMS pour appeler l'API `Encrypt`.
5. CloudTrail envoie deux événements distincts.
   - Un événement est envoyé à Bob. L'événement montre que Bob a utilisé la clé KMS.
   - Un deuxième événement est envoyé à Alice. L'événement montre que Bob a utilisé la clé KMS.
   - Les événements ont les mêmes `sharedEventID`, mais les `eventID` et `recipientAccountID` sont uniques.



Identifiants d'événements partagés dans CloudTrail Insights

Les événements A `sharedEventID` pour CloudTrail Insights sont différents des CloudTrail événements `sharedEventID` relatifs à la gestion et aux types de données. Dans les événements Insights, a `sharedEventID` est un GUID généré par CloudTrail Insights pour identifier de manière unique une paire d'événements Insights de début et de fin. `sharedEventID`Dest courant entre le début et la fin de l'événement Insights et permet de créer une corrélation entre les deux événements afin d'identifier de manière unique les activités inhabituelles.

Vous pouvez considérer `sharedEventID` comme l'ID d'événement Insights global.

CloudTrail Élément UserIdentity

AWS Identity and Access Management (IAM) fournit différents types d'identités. L'élément `userIdentity` contient des détails sur le type d'identité IAM ayant effectué la demande, ainsi que les informations d'identification qui ont été utilisées. Si des informations d'identification temporaires ont été utilisées, l'élément montre comment ces informations d'identification ont été obtenues.

Table des matières

Exemples

`userIdentity` avec les informations d'identification d'utilisateur IAM

L'exemple suivant montre l'élément `userIdentity` d'une demande simple faite avec les informations d'identification de l'utilisateur IAM nommé `Alice`.

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
```

```
  "userName": "Alice"
}
```

`userIdentity` avec des informations d'identification de sécurité temporaires

L'exemple suivant présente un élément `userIdentity` pour une demande faite avec des informations d'identification de sécurité temporaires obtenues en assumant un rôle IAM. L'élément contient des détails supplémentaires concernant le rôle qui a été assumé pour obtenir des informations d'identification.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
    }
}
```

`userIdentity` pour une demande effectuée au nom d'un utilisateur IAM Identity Center

L'exemple suivant présente un élément `userIdentity` pour une demande faite au nom d'un utilisateur IAM Identity Center.

```
"userIdentity": {
 "type": "IdentityCenterUser",
 "accountId": "123456789012",
 "onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
```

```
 },
 "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

Champs

Les champs suivants peuvent apparaître dans un élément `userIdentity`.

`type`

Type d'identité. Les valeurs suivantes sont possibles :

- `Root`— La demande a été faite avec vos Compte AWS informations d'identification. Si le type de `userIdentity` est `Root` et que vous définissez un alias pour votre compte, le champ `userName` contient l'alias de votre compte. Pour plus d'informations, veuillez consulter Votre ID de compte Compte AWS et son alias.
- `IAMUser` - La demande a été effectuée avec les informations d'identification d'un utilisateur IAM.
- `AssumedRole` – La demande a été effectuée avec des informations d'identification de sécurité temporaires qui ont été obtenues avec un rôle en passant un appel à l'API AWS Security Token Service (AWS STS) `AssumeRole`. Cela peut inclure des rôles pour Amazon EC2 et l'accès aux API entre comptes.
- `Role` – La demande a été effectuée avec une identité IAM persistante qui dispose d'autorisations spécifiques. L'émetteur des sessions de rôle est toujours le rôle. Pour plus d'informations sur les rôles, consultez Termes et concepts relatifs aux rôles dans le Guide de l'utilisateur IAM.
- `FederatedUser`— La demande a été faite avec des informations de sécurité temporaires obtenues lors d'un appel à l' AWS STS `GetFederationToken`API. L'élément `sessionIssuer` indique si l'API a été appelée avec les informations d'identification utilisateur racine ou IAM.

  Pour en savoir plus sur les informations d'identification de sécurité temporaires, consultez Informations d'identification de sécurité temporaires dans le Guide de l'utilisateur IAM.
- `Directory` – La demande a été faite à un directory service et le type est inconnu. Les services d'annuaire incluent les suivants : Amazon WorkDocs et Amazon QuickSight.
- `AWSAccount`— La demande a été faite par un autre Compte AWS

- `AWSService`— La demande a été faite par un Compte AWS membre appartenant à un Service AWS. AWS Elastic Beanstalk Suppose, par exemple, un rôle IAM dans votre compte pour appeler d'autres personnes Services AWS en votre nom.
- `IdentityCenterUser` : la demande a été effectuée au nom d'un utilisateur IAM Identity Center.
- `Unknown`— La demande a été faite avec un type d'identité CloudTrail impossible à déterminer.

Facultatif : False

`AWSAccount` et `AWSService` apparaissent pour `type` dans vos journaux lorsqu'il y a un accès entre comptes à l'aide d'un rôle IAM que vous possédez.

Exemple : Accès entre comptes initié par un autre compte AWS

1. Vous possédez un rôle IAM dans votre compte.
2. Un autre AWS compte passe à ce rôle pour assumer le rôle de votre compte.
3. Etant donné que vous possédez le rôle IAM, vous recevez un journal qui indique que l'autre compte a endossé le rôle. Le `type` est `AWSAccount`. Pour un exemple d'entrée de journal, voir événement AWS STS API dans le fichier CloudTrail journal.

Exemple : accès entre comptes initié par un service AWS

1. Vous possédez un rôle IAM dans votre compte.
2. Un AWS compte appartenant à un AWS service assume ce rôle.
3. Etant donné que vous possédez le rôle IAM, vous recevez un journal qui indique que le service AWS a endossé le rôle. Le `type` est `AWSService`.

`userName`

Nom descriptif de l'identité qui a réalisé l'appel. La valeur qui s'affiche dans `userName` s'appuie sur la valeur de `type`. Le tableau suivant illustre la relation entre `type` et `userName` :

`type`	`userName`	Description
`Root` (aucun alias défini)	Absent	Si vous n'avez pas configuré d'alias pour votre Compte AWS, le `userName` champ n'apparaî t pas. Pour plus d'informations sur les alias de

type	userName	Description
		compte, consultez Votre Compte AWS identifiant et son alias. Notez que le champ `userName` ne peut pas contenir `Root`, car `Root` est un type d'identité, et pas un nom d'utilisateur.
`Root` (alias défini)	Alias du compte	Pour plus d'informations sur Compte AWS les alias, consultez la section Votre Compte AWS identifiant et son alias.
`IAMUser`	Nom d'utilisateur de l'utilisateur IAM	
`AssumedRole`	Absent	Pour le type `AssumedRole` , vous trouverez le champ `userName` dans `sessionContext` comme partie de l'élément **`sessionIssuer`** . Pour obtenir un exemple de saisie, consultez Exemples.
`Role`	Défini par l'utilisateur	Les sections `sessionContext` et `sessionIssuer` contiennent des informations concernant l'identité qui a publié la séance pour le rôle.
`FederatedUser`	Absent	Les sections `sessionContext` et `sessionIssuer` contiennent des informations concernant l'identité qui a publié la session pour l'utilisateur fédéré.
`Directory`	Peut être présent	Par exemple, la valeur peut être l'alias du compte ou l'adresse e-mail de l'ID de compte Compte AWS.
`AWSService`	Absent	
`AWSAccount`	Absent	

type	userName	Description
IdentityCenterUser	Absent	La section onBehalfOf contient des informations sur l'ID de l'utilisateur IAM Identity Center et l'ARN du magasin d'identités pour lesquels l'appel a été effectué. Pour plus d'informations sur IAM Identity Center, consultez le Guide de l'utilisateur AWS IAM Identity Center .
Unknown	Peut être présent	Par exemple, la valeur peut être l'alias du compte ou l'adresse e-mail de l'ID de compte Compte AWS.

> **Note**
>
> Le userName contient la chaîne HIDDEN_DUE_TO_SECURITY_REASONS lorsque l'événement enregistré est un échec de connexion à la console provoqué par la saisie d'un nom d'utilisateur incorrect. CloudTrail n'enregistre pas le contenu dans ce cas car le texte peut contenir des informations sensibles, comme dans les exemples suivants :
>
> - Un utilisateur tape par erreur un mot de passe dans le champ de nom d'utilisateur.
> - Un utilisateur clique sur le lien menant à la page de connexion d'un AWS compte, puis saisit le numéro de compte d'un autre compte.
> - Un utilisateur tape accidentellement le nom d'un compte de messagerie personnelle, un identifiant de connexion bancaire ou un autre ID privé.

Facultatif : True

principalId

Identifiant unique de l'entité qui a effectué l'appel. Pour les demandes effectuées avec des informations d'identification de sécurité temporaires, cette valeur comprend le nom de session transmis à l'appel d'API AssumeRole, AssumeRoleWithWebIdentity ou GetFederationToken.

Facultatif : True

`arn`

L'Amazon Resource Name (ARN) du principal qui a effectué l'appel. La dernière partie de l'ARN contient l'utilisateur ou le rôle qui a réalisé l'appel.

Facultatif : True

`accountId`

Compte propriétaire de l'entité qui a accordé les autorisations pour la demande. Si la demande a été effectuée avec des informations d'identification de sécurité temporaires, il s'agit du compte qui possède l'utilisateur ou le rôle IAM utilisé pour obtenir les informations d'identification.

Si la demande a été faite avec un jeton d'accès autorisé IAM Identity Center, il s'agit du compte propriétaire de l'instance IAM Identity Center.

Facultatif : True

`accessKeyId`

ID de clé d'accès utilisé pour signer la demande. Si la demande a été faite avec des informations d'identification de sécurité temporaires, il s'agit de l'ID de clé d'accès des informations d'identification temporaires. Pour des raisons de sécurité,`accessKeyId` peut ne pas être présent ou être affiché sous la forme d'une chaîne vide.

Facultatif : True

`sessionContext`

Si la demande a été effectuée avec les informations d'identification de sécurité temporaires, `sessionContext` fournit des informations sur la session créée pour ces informations d'identification. Une session est créée lorsque vous appelez une API qui renvoie des informations d'identification temporaires. Les utilisateurs créent également des sessions lorsqu'ils travaillent dans la console et font des demandes avec des API qui incluent l'authentification multifactorielle. Cet élément prend en charge les attributs suivants :

- `creationDate` - La date et l'heure auxquelles les informations d'identification de sécurité temporaires ont été émises. Représentées en notation base ISO 8601.
- `mfaAuthenticated` : la valeur est `true` si l'utilisateur root ou l'utilisateur IAM dont les informations d'identification ont été utilisées pour la demande a également été authentifié avec un périphérique MFA. Dans le cas contraire, `false`.
- `sourceIdentity`— Consultez AWS STS identité de la source dans cette rubrique. Le champ `sourceIdentity` se produit dans les événements lorsque les utilisateurs assument

un rôle IAM pour effectuer une action. `sourceIdentity` identifie l'identité de l'utilisateur initial qui effectue la demande, si l'identité de cet utilisateur est un utilisateur IAM, un rôle IAM, un utilisateur authentifié au moyen d'une fédération basée sur SAML ou un utilisateur authentifié à l'aide de la fédération d'identités Web compatible OpenID Connect (OIDC). Pour plus d'informations sur la configuration AWS STS de la collecte des informations d'identité de la source, consultez la section Surveillance et contrôle des actions entreprises avec des rôles assumés dans le Guide de l'utilisateur IAM.

- `ec2RoleDelivery` : la valeur est `1.0` si les informations d'identification ont été fournies par le service Instance Metadata Service Version 1 (IMDSv1) d'Amazon EC2. La valeur est `2.0` si les informations d'identification ont été fournies à l'aide du nouveau schéma IMDS.

  AWS les informations d'identification fournies par le service de métadonnées d'instance Amazon EC2 (IMDS) incluent une clé de contexte ec2 : RoleDelivery IAM. Cette clé de contexte facilite l'application du nouveau schéma sur une resource-by-resource base service-by-service ou en utilisant la clé de contexte comme condition dans les politiques IAM, les politiques de ressources ou les politiques de contrôle des AWS Organizations services. Pour de plus amples informations, consultez Métadonnées d'instance et données utilisateur dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

Facultatif : True

`invokedBy`

Le nom de l'auteur Service AWS de la demande, lorsqu'une demande est faite par un utilisateur Service AWS tel qu'Amazon EC2 Auto Scaling ou. AWS Elastic Beanstalk Ce champ n'est présent que lorsqu'une demande est faite par un Service AWS. Cela inclut les demandes effectuées par des services utilisant des sessions d'accès direct (Service AWS FAS), des principaux, des rôles liés au service ou des rôles de service utilisés par un. Service AWS

Facultatif : True

`sessionIssuer`

Si un utilisateur effectue une demande avec des informations d'identification temporaires, `sessionIssuer` fournit des informations sur la manière dont l'utilisateur a obtenu les informations d'identification. Par exemple, s'il a obtenu des informations d'identification temporaires en endossant un rôle, cet élément fournit des informations sur le rôle endossé. S'ils ont obtenu des informations d'identification avec les informations d'identification de l'utilisateur root ou IAM pour appeler AWS STS `GetFederationToken`, l'élément fournit des informations sur le compte root ou l'utilisateur IAM. Cet élément prend en charge les attributs suivants :

- `type` - La source des informations d'identification de sécurité temporaires, par exemple `Root`, `IAMUser` ou `Role`.
- `userName` - Le nom descriptif de l'utilisateur ou du rôle qui a établi la session. La valeur qui s'affiche dépend du `sessionIssuer` d'identité `type`. Le tableau suivant illustre la relation entre `sessionIssuer type` et `userName` :

`sessionIssuer` type	**`userName`**	Description
`Root` (aucun alias défini)	Absent	Si vous n'avez pas défini d'alias pour votre compte, le champ `userName` n'apparaît pas. Pour plus d'informations sur Compte AWS les alias, consultez la section Votre Compte AWS identifiant et son alias. Notez que le champ `userName` ne peut pas contenir `Root`, car `Root` est un type d'identité, pas un nom d'utilisateur.
`Root` (alias défini)	Alias du compte	Pour plus d'informations sur les Compte AWS alias, consultez la section Votre identifiant de AWS compte et son alias.
`IAMUser`	Le nom d'utilisateur de l'utilisateur IAM	Cela s'applique également lorsqu'un utilisateur fédéré utilise une session établie par `IAMUser`.
`Role`	Nom du rôle	Rôle assumé par un utilisateur IAM ou un utilisateur fédéré par identité Web dans une session de rôle. Service AWS

- `principalId` : l'ID interne de l'entité qui a été utilisée pour obtenir des informations d'identification.
- `arn` - L'ARN de la source (compte, utilisateur IAM ou rôle) qui a été utilisé pour obtenir des informations d'identification de sécurité temporaires.
- `accountId` - Le compte propriétaire de l'entité qui a été utilisée pour obtenir des informations d'identification.

Facultatif : True

`onBehalfOf`

Si la demande a été faite par un appelant IAM Identity Center, `onBehalfOf` fournit des informations sur l'ID de l'utilisateur IAM Identity Center et l'ARN du magasin d'identités pour lesquels l'appel a été effectué. Cet élément prend en charge les attributs suivants :

- `userId` : l'ID de l'utilisateur IAM Identity Center pour lequel l'appel a été effectué.
- `identityStoreArn` : l'ARN du magasin d'identités IAM Identity Center pour lequel l'appel a été effectué.

Facultatif : True

`credentialId`

L'ID des informations d'identification de la demande. Ceci n'est défini que lorsque l'appelant utilise un jeton porteur, tel qu'un jeton d'accès autorisé IAM Identity Center.

Facultatif : True

`webIdFederationData`

Si la demande a été effectuée avec des informations d'identification de sécurité temporaires obtenues par la fédération d'identité Web, `webIdFederationData` répertorie les informations concernant le fournisseur d'identités.

Cet élément prend en charge les attributs suivants :

- `federatedProvider` - Le nom principal du fournisseur d'identités (par exemple, `www.amazon.com` pour Login with Amazon ou `accounts.google.com` pour Google).
- `attributes` - ID d'application et ID d'utilisateur tels qu'indiqués par le fournisseur (par exemple, `www.amazon.com:app_id` et `www.amazon.com:user_id` pour Login with Amazon).

> **Note**
>
> L'omission de ce champ ou la présence de ce champ avec une valeur vide signifie qu'il n'y a aucune information sur le fournisseur d'identité.

Facultatif : True

Valeurs des AWS STS API avec SAML et fédération d'identité Web

AWS CloudTrail prend en charge les appels d'API logging AWS Security Token Service (AWS STS) effectués avec le langage SAML (Security Assertion Markup Language) et la fédération d'identité Web. Lorsqu'un utilisateur appelle les `AssumeRoleWithWebIdentity`API `AssumeRoleWithSAML`et, CloudTrail enregistre l'appel et transmet l'événement à votre compartiment Amazon S3.

L'élément `userIdentity` de ces API contient les valeurs suivantes.

`type`

Type d'identité.

- `SAMLUser` - La demande a été effectuée avec l'assertion SAML.
- `WebIdentityUser` - La demande a été effectuée par un fournisseur de fédération d'identité Web.

`principalId`

Identifiant unique de l'entité qui a effectué l'appel.

- Pour `SAMLUser`, il s'agit d'une combinaison de clés `saml:namequalifier` et `saml:sub`.
- Pour `WebIdentityUser`, il s'agit d'une combinaison de l'émetteur, l'ID de l'application et l'ID de l'utilisateur.

`userName`

Nom de l'identité qui a réalisé l'appel.

- Pour `SAMLUser`, il s'agit de la clé `saml:sub`.
- Pour `WebIdentityUser`, il s'agit de l'ID d'utilisateur.

`identityProvider`

Nom principal du fournisseur d'identité externes. Ce champ s'affiche uniquement pour les types `SAMLUser` ou `WebIdentityUser`.

- Pour `SAMLUser`, il s'agit de la clé `saml:namequalifier` pour l'assertion SAML.
- Pour `WebIdentityUser`, il s'agit du nom d'auteur du fournisseur de fédération d'identité Web. Il peut s'agir d'un fournisseur que vous avez configuré, tel que :

- `cognito-identity.amazon.com` pour Amazon Cognito
- `www.amazon.com` pour Login with Amazon
- `accounts.google.com` pour Google
- `graph.facebook.com` pour Facebook

Voici un exemple d'élément `userIdentity` pour l'action `AssumeRoleWithWebIdentity`.

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

Par exemple, des journaux indiquant la façon dont l'`userIdentity`élément apparaît `SAMLUser` et ses `WebIdentityUser` types, consultez la section Journalisation des appels IAM et AWS STS API avec AWS CloudTrail.

AWS STS identité de la source

Un administrateur IAM peut configurer AWS Security Token Service pour obliger les utilisateurs à spécifier leur identité lorsqu'ils utilisent des informations d'identification temporaires pour assumer des rôles. Le champ `sourceIdentity` apparait dans les événements lorsque les utilisateurs assument un rôle IAM ou exécutent des actions avec le rôle assumé.

Le `sourceIdentity` identifie l'identité de l'utilisateur d'origine qui effectue la demande, si l'identité de cet utilisateur est un utilisateur IAM, un rôle IAM, un utilisateur authentifié à l'aide de la fédération basée sur SAML ou un utilisateur authentifié à l'aide de la fédération d'identités Web compatible OpenID Connect (OIDC). Une fois que l'administrateur IAM a configuré AWS STS, CloudTrail enregistre les `sourceIdentity` informations relatives aux événements et aux emplacements suivants dans l'enregistrement des événements :

- Le ou AWS STS `AssumeRole` `AssumeRoleWithSAML` les `AssumeRoleWithWebIdentity` appels qu'une identité d'utilisateur effectue lorsqu'elle assume un rôle. `sourceIdentity`se trouve dans le `requestParameters` bloc des AWS STS appels.
- Le ou AWS STS `AssumeRole` les `AssumeRoleWithSAML` `AssumeRoleWithWebIdentity` appels qu'une identité d'utilisateur effectue si elle utilise un rôle pour assumer un autre

rôle, c'est ce que l'on appelle le chaînage de rôles. `sourceIdentity`se trouve dans le `requestParameters` bloc des AWS STS appels.

- L'API AWS de service effectue les appels que l'identité de l'utilisateur effectue lorsqu'il assume un rôle et en utilisant les informations d'identification temporaires attribuées par AWS STS. Dans les événements d'API de service, `sourceIdentity` se trouve dans le bloc `sessionContext`. Par exemple, si une identité utilisateur crée un nouveau compartiment S3, `sourceIdentity` se produit dans le bloc `sessionContext`de l'événement `CreateBucket`.

Pour plus d'informations sur la façon de configurer AWS STS la collecte des informations d'identité source, consultez la section Surveillance et contrôle des actions entreprises avec des rôles assumés dans le Guide de l'utilisateur IAM. Pour plus d'informations sur les AWS STS événements auxquels vous êtes connecté CloudTrail, consultez la section Journalisation des appels IAM et AWS STS API AWS CloudTrail dans le guide de l'utilisateur IAM.

Les exemples suivants sont des extraits d'événements qui montrent la `sourceIdentity`.

Exemple de la section **`requestParameters`**

Dans l'exemple d'extrait d'événement suivant, un utilisateur fait une AWS STS `AssumeRole` demande et définit une identité source, représentée ici par. *`source-identity-value-set`* L'utilisateur assume un rôle représenté par le rôle ARN `arn:aws:iam::123456789012:role/Assumed_Role`. Le champ `sourceIdentity` se trouve dans le bloc `requestParameters` de l'événement.

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
```

```
    },
```

Exemple de la section **`responseElements`**

Dans l'exemple d'extrait d'événement suivant, un utilisateur AWS STS `AssumeRole` demande à assumer un rôle nommé `Developer_Role` et définit une identité source. `Admin` L'utilisateur assume un rôle représenté par le rôle ARN `arn:aws:iam::111122223333:role/Developer_Role`. Le champ `sourceIdentity` est affiché à la fois dans les blocs `requestParameters` et `responseElements` de l'événement. Les informations d'identification temporaires utilisées pour assumer le rôle, la chaîne de jeton de session, ainsi que l'ID de rôle assumé, le nom de session et l'ARN de session sont affichés dansle bloc `responseElements`, ainsi que l'identité source.

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                            EXAMPLE_SESSION_TOKEN
                            XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

Exemple de la section **`sessionContext`**

Dans l'exemple d'extrait d'événement suivant, un utilisateur assume un rôle nommé `DevRole` pour appeler une API de AWS service. L'utilisateur définit une identité source, représentée ici par *`source-identity-value-set`*. Le champ `sourceIdentity` se trouve dans le bloc `sessionContext`, à l'intérieur du bloc `userIdentity` de l'événement.

```
{
```

```
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

CloudTrail **`insightDetails`**Élément Insights

AWS CloudTrail Les enregistrements d'événements Insights incluent des champs différents des autres CloudTrail événements de leur structure JSON, parfois appelés charge utile. Un enregistrement d'événement CloudTrail Insights inclut un `insightDetails` bloc contenant des informations sur les déclencheurs sous-jacents d'un événement Insights, telles que la source de l'événement, les identités des utilisateurs, les agents utilisateurs, les moyennes ou les valeurs de référence historiques, les statistiques, le nom de l'API, et si l'événement marque le début ou la fin de l'événement Insights. Le bloc `insightDetails` contient les informations suivantes :

- **`state`** - Indique si l'événement constitue l'événement Insights de début ou de fin. La valeur peut être `Start` ou `End`.

  Depuis : 1.07

  Facultatif : False

- **`eventSource`**- Le point AWS de terminaison du service à l'origine de l'activité inhabituelle, tel que`ec2.amazonaws.com`.

  Depuis : 1.07

  Facultatif : False

- **`eventName`** - Le nom de l'événement Insights, généralement le nom de l'API qui était la source de l'activité inhabituelle.

  Depuis : 1.07

  Facultatif : False

- **`insightType`** - Le type de l'événement Insights. Cette valeur peut être `ApiCallRateInsight`, `ApiErrorRateInsight` ou les deux.

  Depuis : 1.07

  Facultatif : False

- **`insightContext`** -

  Informations sur les AWS outils (appelés agents utilisateurs), les utilisateurs et les rôles IAM (appelés identités d'utilisateurs) et les codes d'erreur associés aux événements CloudTrail analysés pour générer l'événement Insights. Cet élément inclut également des statistiques montrant comment l'activité inhabituelle d'un événement Insights se compare à l'activité de référence, ou normale.

  Depuis : 1.07

  Facultatif : False

  - **`statistics`** - Inclut des données sur la baseline (référence), ou taux moyen général d'appels vers l'API objet par un compte tel que mesuré pendant la période de référence, le taux moyen d'appels ayant déclenché l'événement Insights pendant la première minute de l'événement Insights, la durée, en minutes, de l'événement Insights, et la durée, en minutes, de la période de mesure de référence.

    Depuis : 1.07

    Facultatif : False

- **`baseline`** - Le nombre moyen d'appels d'API ou d'erreurs par minute pendant la durée de référence sur l'API objet de l'événement Insights pour le compte, calculé sur les sept jours précédant le début de l'événement Insights.

  Depuis : 1.07

  Facultatif : False

- **`insight`** -

  Pour un événement Insights de démarrage, cette valeur correspond au nombre moyen d'appels d'API ou d'erreurs par minute au début de l'activité inhabituelle. Pour un événement Insights de fin, cette valeur correspond au nombre moyen d'appels d'API ou d'erreurs par minute pendant la durée de l'activité inhabituelle.

  Depuis : 1.07

  Facultatif : False

- **`insightDuration`** - La durée, en minutes, d'un événement Insights (période comprise entre le début et la fin d'une activité inhabituelle sur l'API objet). `insightDuration` se produit au début et à la fin des événements Insights.

  Depuis : 1.07

  Facultatif : False

- **`baselineDuration`** - La durée, en minutes, de la période de référence (période pendant laquelle l'activité normale est mesurée sur l'API objet). `baselineDuration` correspond au minimum aux sept jours (10 080 minutes) précédant un événement Insights. Ce champ se produit dans les événements Insights de début et de fin. L'heure de fin de la mesure `baselineDuration` correspond toujours au démarrage d'un événement Insights.

  Depuis : 1.07

  Facultatif : False

- **`attributions`**- Ce bloc contient des informations sur les identités utilisateur, les agents utilisateur et les codes d'erreur en corrélation avec une activité inhabituelle et de référence. Un maximum de cinq identités utilisateur, cinq agents utilisateur et cinq codes d'erreur sont capturés dans un bloc `attributions` d'événement Insights, trié par une moyenne du nombre d'activités, dans l'ordre décroissant du plus élevé au plus bas.

Depuis : 1.07

Facultatif : True

- **`attribute`**- Contient le type d'attribut. La valeur peut être définie à `userIdentityArn`, `userAgent` ou `errorCode`.
  - **`userIdentityArn`**- Un bloc répertoriant les cinq principaux AWS utilisateurs ou rôles IAM ayant contribué aux appels ou aux erreurs d'API au cours de l'activité inhabituelle et des périodes de référence. Consultez aussi `userIdentity` dans CloudTrail enregistrer le contenu.

    Depuis : 1.07

    Facultatif : False
    - **`insight`**- Un bloc qui affiche jusqu'aux cinq ARN d'identité utilisateur qui ont contribué aux appels d'API effectués pendant la période d'activité inhabituelle, dans l'ordre décroissant du nombre d'appels d'API le plus élevé au plus petit. Il indique également le nombre moyen d'appels d'API effectués par les identités d'utilisateur au cours de la période d'activité inhabituelle.

      Depuis : 1.07

      Facultatif : False
      - **`value`**- L'ARN de l'une des cinq principales identités utilisateur qui ont contribué aux appels d'API effectués au cours de la période d'activité inhabituelle.

        Depuis : 1.07

        Facultatif : False
      - **`average`** - Le nombre d'appels d'API ou d'erreurs par minute au cours de la période d'activité inhabituelle pour l'identité utilisateur dans le champ `value`.

        Depuis : 1.07

        Facultatif : False
    - **`baseline`** - Un bloc qui affiche jusqu'aux cinq ARN d'identité utilisateur qui ont le plus contribué aux appels d'API ou d'erreurs effectués pendant la période d'activité normale. Il indique également le nombre moyen d'appels d'API ou d'erreurs journalisés par les identités utilisateur au cours de la période d'activité normale.

Depuis : 1.07

Facultatif : False

- **`value`** - L'ARN de l'une des cinq principales identités utilisateur qui ont contribué aux appels d'API ou erreurs effectués pendant la période d'activité normale.

  Depuis : 1.07

  Facultatif : False

- **`average`** - La moyenne antérieure des appels d'API ou erreurs par minute au cours des sept jours précédant l'heure de démarrage de l'activité Insights pour l'identité utilisateur dans le champ `value`.

  Depuis : 1.07

  Facultatif : False

- **`userAgent`**- Un bloc qui affiche les cinq principaux AWS outils par lesquels l'identité de l'utilisateur a contribué aux appels d'API pendant les périodes d'activité inhabituelle et de référence. Ces outils incluent le AWS Management Console AWS CLI, ou les AWS SDK. Consultez aussi `userAgent` dans CloudTrail enregistrer le contenu.

  Depuis : 1.07

  Facultatif : False

  - **`insight`** - Un bloc qui affiche jusqu'aux cinq principaux agents utilisateur qui ont contribué aux appels d'API effectués pendant la période d'activité inhabituelle, dans l'ordre décroissant du plus nombre d'appels d'API le plus élevé au plus petit. Il indique également le nombre moyen d'appels d'API ou d'erreurs journalisés par les agents utilisateur au cours de la période d'activité inhabituelle.

    Depuis : 1.07

    Facultatif : False

    - **`value`** - L'un des cinq principaux agents utilisateur qui ont contribué aux appels d'API effectués au cours de la période d'activité inhabituelle.

      Depuis : 1.07

Facultatif : False

- **`average`** - Le nombre d'appels d'API ou d'erreurs journalisés par minute au cours de la période d'activité inhabituelle pour l'agent utilisateur dans le champ `value`.

  Depuis : 1.07

  Facultatif : False

- **`baseline`** - Un bloc qui affiche jusqu'aux cinq principaux agents utilisateur qui ont le plus contribué aux appels d'API effectués pendant la période d'activité normale. Il indique également le nombre moyen d'appels d'API ou d'erreurs journalisés par les agents utilisateur au cours de la période d'activité normale.

  Depuis : 1.07

  Facultatif : False

  - **`value`** - L'un des cinq principaux agents utilisateur qui ont contribué aux appels d'API ou erreurs journalisés pendant la période d'activité normale.

    Depuis : 1.07

    Facultatif : False

  - **`average`** - La moyenne antérieure des appels d'API ou erreurs par minute au cours des sept jours précédant l'heure de démarrage de l'activité Insights pour l'agent utilisateur dans le champ `value`.

    Depuis : 1.07

    Facultatif : False

- **`errorCode`** - Un bloc qui affiche jusqu'aux cinq premiers codes d'erreur qui se sont produits sur les appels d'API pendant les périodes d'activité inhabituelles et de référence, dans l'ordre décroissant du nombre d'appels d'API le plus élevé au plus petit. Consultez aussi `errorCode` dans CloudTrail enregistrer le contenu.

  Depuis : 1.07

  Facultatif : False

  - **`insight`** - Un bloc qui affiche jusqu'aux cinq premiers codes d'erreur qui se sont produits sur les appels d'API effectués pendant la période d'activité inhabituelle, dans l'ordre

décroissant du nombre d'appels d'API le plus élevé au plus petit. Il indique également le nombre moyen d'appels d'API sur lesquels les erreurs se sont produites au cours de la période d'activité inhabituelle.

Depuis : 1.07

Facultatif : False

- **`value`** - L'un des cinq principaux codes d'erreur qui se sont produits sur les appels API effectués pendant la période d'activité inhabituelle, tels que `AccessDeniedException`.

  Si aucun des appels qui ont déclenché l'événement Insights n'a entraîné d'erreurs, cette valeur est définie à `null`.

  Depuis : 1.07

  Facultatif : False

- **`average`** - Le nombre d'appels API par minute au cours de la période d'activité inhabituelle pour le code d'erreur dans le champ `value`.

  Si la valeur du code d'erreur est définie à `null`, et il n'y a pas d'autres codes d'erreur dans le bloc `insight`, la valeur de la propriété `average` est identique à celle de la `statistics` pour l'événement Insights dans son ensemble.

  Depuis : 1.07

  Facultatif : False

- **`baseline`** - Un bloc qui affiche jusqu'aux cinq premiers codes d'erreur qui se sont produits sur les appels d'API effectués pendant la période d'activité normale. Il indique également le nombre moyen d'appels d'API effectués par les agents utilisateur au cours de la période d'activité normale.

  Depuis : 1.07

  Facultatif : False

  - **`value`** - L'un des cinq principaux codes d'erreur qui se sont produits sur les appels d'API effectués pendant la période d'activité normale, tels que `AccessDeniedException`.

Depuis : 1.07

Facultatif : False

- **`average`** - La moyenne antérieure des appels d'API ou d'erreurs par minute au cours des sept jours précédant l'heure de démarrage de l'activité Insights pour le code d'erreur dans le champ `value`.

  Depuis : 1.07

  Facultatif : False

Exemple bloc **`insightDetails`**

Voici un exemple de bloc `insightDetails` d'événement Insights pour un événement Insights qui s'est produit lorsque l'API Application Auto Scaling `CompleteLifecycleAction` été appelée un nombre inhabituel de fois. Pour obtenir un exemple d'événement Insights complet, consultez Événements Insights.

Cet exemple provient d'un événement Insights de démarrage, indiqué par `"state": "Start"`. Les identités utilisateur les plus importantes qui ont appelé les API associées à l'événement Insights,`CodeDeployRole1`, `CodeDeployRole2`, et `CodeDeployRole3`, sont indiqués dans le bloc `attributions`, ainsi que leurs taux d'appels d'API moyens pour cet événement Insights, et la référence pour le rôle `CodeDeployRole1`. Le `attributions` bloc indique également que l'agent utilisateur l'est`codedeploy.amazonaws.com`, ce qui signifie que les principales identités d'utilisateurs ont utilisé la AWS CodeDeploy console pour exécuter les appels d'API.

Parce qu'aucun code d'erreur n'est associé aux événements qui ont été analysés pour générer l'événement Insights (la valeur est définie à `null`), la moyenne `insight` pour le code d'erreur est la même que la moyenne générale `insight`pour l'ensemble de l'événement Insights, illustrée dans le bloc `statistics`.

```
        "insightDetails": {
          "state": "Start",
          "eventSource": "autoscaling.amazonaws.com",
          "eventName": "CompleteLifecycleAction",
          "insightType": "ApiCallRateInsight",
          "insightContext": {
            "statistics": {
              "baseline": {
```

```
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "userAgent",
                  "insight": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.6
                    }
                  ],
```

```
            "baseline": [
              {
                "value": "codedeploy.amazonaws.com",
                "average": 0.0000882145
              }
            ]
          },
          {
            "attribute": "errorCode",
            "insight": [
              {
                "value": "null",
                "average": 0.6
              }
            ],
            "baseline": [
              {
                "value": "null",
                "average": 0.0000882145
              }
            ]
          }
        ]
      }
    }
```

Événements non liés à l'API capturés par CloudTrail

Outre la journalisation des appels d' AWS API, CloudTrail capture d'autres événements connexes susceptibles d'avoir un impact sur la sécurité ou la conformité de votre AWS compte ou de vous aider à résoudre des problèmes opérationnels.

Rubriques

- AWS événements de service
- AWS Management Console événements de connexion

AWS événements de service

CloudTrail prend en charge la journalisation des événements de service autres que les API. Ces événements sont créés par les AWS services mais ne sont pas directement déclenchés par une

demande adressée à une AWS API publique. Pour ces événements, le champ `eventType` est `AwsServiceEvent`.

Voici un exemple de scénario d'événement de AWS service dans lequel une clé gérée par le client est automatiquement déplacée vers AWS Key Management Service (AWS KMS). Pour plus d'informations sur la rotation des clés, consultez Rotating KMS keys (Rotation des clés KMS).


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```


AWS Management Console événements de connexion

CloudTrail enregistre les tentatives de connexion aux AWS Management Console forums de AWS discussion et au Centre de AWS support. Tous les événements de connexion des utilisateurs IAM et des utilisateurs root, ainsi que tous les événements de connexion des utilisateurs fédérés,

générent des enregistrements dans des fichiers journaux. CloudTrail Pour plus d'informations sur la recherche et l'affichage des journaux, veuillez consulter Trouver vos fichiers CloudTrail journaux et Téléchargement de vos fichiers CloudTrail journaux.

> **Note**
>
> La région enregistrée `ConsoleLogin` lors d'un événement varie en fonction du type d'utilisateur et du fait que vous utilisiez un point de terminaison mondial ou régional pour vous connecter.
>
> - Si vous vous connectez en tant qu'utilisateur root, CloudTrail enregistre l'événement dans us-east-1.
> - Si vous vous connectez avec un utilisateur IAM et que vous utilisez le point de terminaison global CloudTrail , enregistrez la région de l'`ConsoleLogin`événement comme suit :
>   - Si un cookie d'alias de compte est présent dans le navigateur, il CloudTrail enregistre l'`ConsoleLogin`événement dans l'une des régions suivantes : us-east-2, eu-north-1 ou ap-southeast-2. Cela est dû au fait que le proxy de console redirige l'utilisateur en fonction de la latence depuis l'emplacement de connexion de l'utilisateur.
>   - Si aucun cookie d'alias de compte n'est présent dans le navigateur, CloudTrail enregistre l'`ConsoleLogin`événement dans us-east-1. Cela est dû au fait que le proxy de console redirige vers la connexion globale.
> - Si vous vous connectez avec un utilisateur IAM et utilisez un point de terminaison régional, CloudTrail enregistre l'`ConsoleLogin`événement dans la région appropriée pour le point de terminaison. Pour plus d'informations sur les points de Connexion à AWS terminaison, consultez la section Points de Connexion à AWS terminaison et quotas.

Rubriques

Exemple d'enregistrements d'événements pour les utilisateurs IAM

Les exemples suivants illustrent les enregistrements d'événements pour plusieurs scénarios de connexion d'utilisateur IAM.

Rubriques

Utilisateur IAM, connexion réussie sans MFA

L'enregistrement suivant indique qu'un utilisateur nommé s'est connecté `Anaya` avec succès au AWS Management Console sans utiliser l'authentification multifactorielle (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
```

```
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


Utilisateur IAM, connexion réussie avec MFA

L'enregistrement suivant montre qu'un utilisateur IAM nommé s'est connecté `Anaya` avec succès à l' AWS Management Console aide de l'authentification multifactorielle (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
```

```
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Utilisateur IAM, échec de connexion

L'enregistrement suivant montre l'échec d'une tentative de connexion d'un utilisateur IAM nommé `Paulo`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
```

```
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


Utilisateur IAM, le processus de connexion vérifie la nécessité d'une MFA (type de périphérique MFA unique)

L'exemple suivant montre que le processus du connexion a vérifié si l'authentification multifacteur (MFA), est requise pour un utilisateur IAM lors de la connexion. Dans cet exemple, la valeur de `mfaType` est `U2F MFA`, ce qui indique que l'utilisateur IAM a activé soit un seul périphérique MFA, soit plusieurs périphériques MFA du même type (`U2F MFA`).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
```

```
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Utilisateur IAM, le processus de connexion vérifie la nécessité d'une MFA (plusieurs types de périphériques MFA)

L'exemple suivant montre que le processus du connexion a vérifié si l'authentification multifacteur (MFA), est requise pour un utilisateur IAM lors de la connexion. Dans cet exemple, la valeur `mfaType` est `Multiple MFA Devices`, ce qui indique que l'utilisateur IAM a activé plusieurs types de périphériques MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Mary"
    },
    "eventTime": "2023-07-19T23:10:09Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
```

```
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Multiple MFA Devices"
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Exemple d'enregistrements d'événements pour les utilisateurs racine

Les exemples suivants montrent les enregistrements d'événements pour plusieurs scénarios de connexion d'utilisateur `root`. Lorsque vous vous connectez en utilisant l'utilisateur root, CloudTrail enregistre l'`ConsoleLogin`événement dans us-east-1.

Rubriques

- Utilisateur racine, connexion réussie sans MFA
- Utilisateur racine, connexion réussie avec MFA
- Utilisateur racine, échec de connexion
- Utilisateur racine, MFA modifié
- Utilisateur racine, mot de passe modifié

Utilisateur racine, connexion réussie sans MFA

L'exemple suivant illustre un événement de connexion réussie pour un utilisateur racine qui n'utilise pas l'authentification multifactorielle (MFA).

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


Utilisateur racine, connexion réussie avec MFA

L'exemple suivant illustre un événement de connexion réussie pour un utilisateur racine qui utilise l'authentification multifactorielle (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Utilisateur racine, échec de connexion

L'exemple suivant illustre un événement d'échec de connexion pour un utilisateur racine qui n'utilise pas MFA.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
```

```
}
```

Utilisateur racine, MFA modifié

L'exemple suivant montre un événement décrivant un utilisateur racine qui modifie les paramètres d'authentification multifacteur (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Utilisateur racine, mot de passe modifié

L'exemple suivant montre un événement décrivant un utilisateur racine qui modifie son mot de passe.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
}
```

Exemple d'enregistrements d'événements pour les utilisateurs fédérés

Les exemples suivants illustrent les enregistrements d'événements pour les utilisateurs fédérés. Les utilisateurs fédérés reçoivent des informations d'identification de sécurité temporaires leur permettant d'accéder aux AWS ressources par le biais d'une `AssumeRole`demande.

L'exemple suivant montre un événement décrivant une demande de chiffrement de fédération. L'ID de clé d'accès d'origine est fourni dans le champ `accessKeyId` de l'élément `userIdentity`. Le champ `accessKeyId` de l'élément `responseElements` contient un nouvel identifiant de clé d'accès si la demande `sessionDuration` est transmise dans la demande de chiffrement, sinon il contient la valeur de l'identifiant de clé d'accès d'origine.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
```

```
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

L'exemple suivant illustre un événement de connexion réussie pour un utilisateur fédéré qui n'utilise pas l'authentification multifactorielle (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Utilisation de fichiers CloudTrail journaux

Vous pouvez effectuer des tâches plus avancées avec vos CloudTrail fichiers.

- Créer plusieurs journaux de suivi par région.
- Surveillez les fichiers CloudTrail journaux en les envoyant à CloudWatch Logs.
- Partager des fichiers journaux entre les comptes.
- Utilisez la bibliothèque AWS CloudTrail de traitement pour écrire des applications de traitement des journaux en Java.
- Validez vos fichiers journaux pour vérifier qu'ils n'ont pas changé après leur livraison CloudTrail.

Lorsqu'un événement se produit dans votre compte, CloudTrail évalue si l'événement correspond aux paramètres de vos sentiers. Seuls les événements correspondant à vos paramètres de suivi sont transmis à votre compartiment Amazon S3 et à votre groupe de CloudWatch journaux Amazon Logs.

Vous pouvez configurer plusieurs journaux d'activité différemment pour que ceux-ci traitent et journalisent uniquement les événements que vous spécifiez. Par exemple, un journal d'activité peut journaliser les événements de données et de gestion en lecture seule, de sorte que tous les événements en lecture seule soient livrés à un compartiment S3. Un autre journal d'activité peut journaliser uniquement les événements de gestion et de données en écriture seule, de sorte que tous les événements en écriture seule soient livrés à un compartiment S3 distinct.

Vous pouvez également configurer vos journaux d'activité pour que l'un des suivis livre tous les événements de gestion dans un compartiment S3 et qu'un autre suivi livre tous les événements de données dans un autre compartiment S3.

Vous pouvez configurer vos journaux d'activité pour journaliser les éléments suivants :

- Événements de données : ces événements fournissent des informations sur les opérations de ressource exécutées sur ou dans une ressource. Ils sont également connus sous le nom d'opérations de plans de données.
- Événements de gestion : les événements de gestion fournissent une visibilité sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom d'opérations de plan de contrôle. Les événements de gestion peuvent aussi inclure les événements non API qui se produisent dans votre compte. Par exemple, lorsqu'un utilisateur se connecte à votre compte, CloudTrail enregistre l'`ConsoleLogin`événement. Pour plus d'informations, consultez Événements non liés à l'API capturés par CloudTrail.

- Événements Insights : les événements Insights capturent l'activité inhabituelle qui est détectée dans votre compte. Si les événements Insights sont activés et que vous CloudTrail détectez une activité inhabituelle, les événements Insights sont enregistrés dans le compartiment S3 de destination pour votre parcours, mais dans un dossier différent. Vous pouvez également voir le type d'événement Insights et la période de l'incident lorsque vous consultez les événements Insights sur la CloudTrail console. Contrairement aux autres types d'événements capturés lors d'un CloudTrail suivi, les événements Insights sont enregistrés uniquement lorsque des modifications de l'utilisation de l'API de votre compte sont CloudTrail détectées et qu'elles diffèrent considérablement des modèles d'utilisation habituels du compte.

  Les événements Insights sont générés uniquement pour les API de gestion. Pour plus d'informations, consultez Journalisation des événements Insights.

> **Note**
>
> CloudTrail fournit généralement des journaux dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti. Pour plus d'informations, consultez le Contrat de niveau de service (SLA)AWS CloudTrail.
> Si vous configurez mal votre trace (par exemple, si le compartiment S3 est inaccessible), vous CloudTrail tenterez de remettre les fichiers journaux à votre compartiment S3 pendant 30 jours, et ces attempted-to-deliver événements seront soumis aux frais standard. CloudTrail Pour éviter des frais sur un journal de suivi mal configuré, vous devez supprimer le journal de suivi.

Rubriques

Réception de fichiers CloudTrail journaux provenant de plusieurs régions

Vous pouvez configurer CloudTrail pour fournir des fichiers journaux provenant de plusieurs régions vers un seul compartiment S3 pour un seul compte. Par exemple, vous avez un parcours dans la région de l'ouest des États-Unis (Oregon) configuré pour envoyer des fichiers journaux à un compartiment S3, ainsi qu'un groupe de CloudWatch journaux Logs. Lorsque vous modifiez un journal régional existant pour enregistrer toutes les régions, CloudTrail enregistre les événements de toutes les régions qui se trouvent sur une seule AWS partition de votre compte. CloudTrail fournit les fichiers journaux au même compartiment S3 et au même groupe de CloudWatch journaux Logs. Tant CloudTrail que vous êtes autorisé à écrire dans un compartiment S3, le compartiment d'un sentier multirégional ne doit pas nécessairement se trouver dans la région d'origine du sentier.

Pour enregistrer les événements de toutes les régions dans toutes les AWS partitions de votre compte, créez un journal multirégional dans chaque partition.

Dans la console, vous créez par défaut un journal de suivi qui journalise les événements dans toutes les Régions AWS de la partition AWS dans laquelle vous opérez. Il s'agit d'une bonne pratique recommandée. Pour journaliser les événements dans une région unique (non recommandé), utilisez l' AWS CLI. Pour configurer un journal de suivi à région unique existant pour journaliser toutes les régions, vous devez utiliser l' AWS CLI.

Pour modifier un journal d'activités existant afin qu'il s'applique à toutes les régions, il convient d'ajouter l'option `--is-multi-region-trail` à la commande update-trail.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Afin de confirmer que le journal d'activité s'applique maintenant à toutes les régions, l'élément `IsMultiRegionTrail` dans le résultat affiche `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Lorsqu'une nouvelle région est lancée dans la awspartition, elle crée CloudTrail automatiquement un parcours pour vous dans la nouvelle région avec les mêmes paramètres que votre parcours d'origine.

Pour plus d'informations, consultez les ressources suivantes :

- Travailler avec les CloudTrail sentiers
- CloudTrail FAQ

Gérer la cohérence des données dans CloudTrail

CloudTrail utilise un modèle informatique distribué appelé cohérence éventuelle. Toute modification apportée à votre CloudTrail configuration (ou à d'autres AWS services), y compris les balises utilisées dans le contrôle d'accès basé sur les attributs (ABAC), met du temps à être visible depuis tous les points de terminaison possibles. Ce retard est dû en partie au temps nécessaire pour envoyer les données d'un serveur à un autre, d'une zone de réplication à une autre et d'une région à l'autre dans le monde entier. CloudTrail utilise également la mise en cache pour améliorer les performances, mais dans certains cas, cela peut ajouter du temps. La modification peut ne pas être visible tant que les données mises en cache précédemment n'arrivent pas à expiration.

Vous devez concevoir vos applications de sorte qu'elles tiennent compte de ces retards potentiels. Assurez-vous qu'elles fonctionnent comme prévu, même lorsqu'une modification effectuée à un emplacement n'est pas visible instantanément à un autre. Ces modifications incluent la création ou la mise à jour de journaux de suivi ou de stockages de données d'événement, la mise à jour de sélecteurs d'événements et le démarrage ou l'arrêt de la journalisation. Lorsque vous créez ou mettez à jour un magasin de données de suivi ou d'événement, les CloudTrail journaux sont transmis au compartiment S3 ou au magasin de données d'événements en fonction de la dernière configuration connue jusqu'à ce que les modifications se propagent à tous les emplacements.

Pour plus d'informations sur la façon dont cela affecte les autres Services AWS, consultez les ressources suivantes :

- Amazon DynamoDB : les sections En quoi consiste le modèle de cohérence de DynamoDB ? de la Questions fréquentes (FAQ) sur DynamoDB, et Cohérence en lecture du Guide du développeur Amazon DynamoDB.

- Amazon EC2 : section Cohérence à terme (français non garanti) de la Référence d'API Amazon Elastic Compute Cloud.
- Amazon EMR : garantir la cohérence lors de l'utilisation d'Amazon S3 et d'Amazon Elastic MapReduce pour les flux de travail ETL sur le blog AWS Big Data.
- AWS Identity and Access Management (IAM) : Les modifications que j'apporte ne sont pas toujours immédiatement visibles dans le guide de l'utilisateur IAM.
- Amazon Redshift : section Gestion de la cohérence des données du Guide du développeur de base de données Amazon Redshift.
- Amazon S3 : section Modèle de cohérence des données Amazon S3 du Guide de l'utilisateur Amazon Simple Storage Service.

Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs

Vous pouvez configurer CloudTrail les CloudWatch journaux pour surveiller vos journaux de suivi et être averti lorsqu'une activité spécifique se produit.

1. Configurez votre suivi pour envoyer les événements du journal à CloudWatch Logs.
2. Définissez CloudWatch les filtres métriques des journaux pour évaluer les événements des journaux afin de détecter des correspondances en termes, phrases ou valeurs. Par exemple, vous pouvez contrôler les événements `ConsoleLogin`.
3. Attribuez CloudWatch des métriques aux filtres de métriques.
4. Créez des CloudWatch alarmes déclenchées en fonction des seuils et des périodes que vous spécifiez. Vous pouvez configurer des alarmes pour envoyer des notifications lorsqu'elles sont déclenchées, de manière à ce que vous puissiez agir.
5. Vous pouvez également configurer CloudWatch pour exécuter automatiquement une action en réponse à une alarme.

La tarification standard pour Amazon CloudWatch et Amazon CloudWatch Logs s'applique. Pour plus d'informations, consultez Amazon CloudWatch Pricing.

Pour plus d'informations sur les régions dans lesquelles vous pouvez configurer vos parcours pour envoyer des CloudWatch journaux à Logs, consultez la section Régions et quotas Amazon CloudWatch Logs dans le manuel de référence AWS général.

Rubriques

Envoyer des événements à CloudWatch Logs

Lorsque vous configurez votre parcours pour envoyer des événements à CloudWatch Logs, il CloudTrail envoie uniquement les événements correspondant à vos paramètres de suivi. Par exemple, si vous configurez votre journal pour qu'il enregistre uniquement les événements liés aux données, il envoie les événements de données uniquement à votre groupe de CloudWatch journaux Logs. CloudTrail prend en charge l'envoi de données, d'informations et d'événements de gestion vers CloudWatch Logs. Pour plus d'informations, consultez Utilisation de fichiers CloudTrail journaux.

> **Note**
>
> Seul le compte de gestion peut configurer un groupe de CloudWatch journaux pour un journal d'entreprise à l'aide de la console. L'administrateur délégué peut configurer un groupe de CloudWatch journaux Logs à l'aide des opérations AWS CLI CloudTrail `CreateTrail` ou de `UpdateTrail` l'API.

Pour envoyer des événements à un groupe de CloudWatch journaux Logs :

- Vérifiez que vous disposez des autorisations suffisantes pour créer ou spécifier un rôle IAM. Pour plus d'informations, consultez Octroi de l'autorisation d'afficher et de configurer CloudWatch les informations Amazon Logs sur la CloudTrail console.
- Si vous configurez le groupe de CloudWatch journaux à l'aide du AWS CLI, assurez-vous de disposer des autorisations suffisantes pour créer un flux de CloudWatch journaux journaux dans le groupe de journaux que vous spécifiez et pour transmettre des CloudTrail événements à ce flux de journaux. Pour plus d'informations, consultez Création d'un document de politique.
- Créez un journal d'activité ou sélectionnez un journal d'activité existant. Pour plus d'informations, consultez Création et mise à jour d'un journal d'activité à l'aide de la console.

- Créez un groupe de journaux ou indiquez-en un existant.
- Spécifiez un rôle IAM. Si vous modifiez un rôle IAM existant pour un journal d'activité de l'organisation, vous devez mettre à jour manuellement la politique de façon à autoriser la journalisation du journal d'activité de l'organisation. Pour plus d'informations, consultez cet exemple de politique et Création d'un journal de suivi pour une organisation.
- Attachez une politique de rôle ou utilisez la politique par défaut.

Table des matières

Configuration de la surveillance des CloudWatch journaux avec la console

Vous pouvez utiliser le AWS Management Console pour configurer votre journal afin d'envoyer des événements aux CloudWatch journaux à des fins de surveillance.

Création d'un groupe de journaux ou spécification d'un groupe de journaux existant

CloudTrail utilise un groupe de CloudWatch journaux comme point de terminaison de livraison pour les événements du journal. Vous pouvez créer un groupe de journaux ou spécifier un groupe existant.

Pour créer ou spécifier un groupe de journaux pour un suivi existant

1. Assurez-vous de vous connecter avec un utilisateur ou un rôle administratif disposant des autorisations suffisantes pour configurer l'intégration CloudWatch des journaux. Pour plus

d'informations, consultez Octroi de l'autorisation d'afficher et de configurer CloudWatch les informations Amazon Logs sur la CloudTrail console.

> **Note**
>
> Seul le compte de gestion peut configurer un groupe de CloudWatch journaux pour un journal d'entreprise à l'aide de la console. L'administrateur délégué peut configurer un groupe de CloudWatch journaux Logs à l'aide des opérations AWS CLI CloudTrail `CreateTrail` ou de `UpdateTrail` l'API.

2. Ouvrez la CloudTrail console à l'adresse https://console.aws.amazon.com/cloudtrail/.
3. Choisissez le nom du journal d'activité. Si vous sélectionnez un suivi qui s'applique à toutes les régions, vous serez redirigé vers la région où le journal de suivi a été créé. Vous pouvez créer un groupe de journaux ou choisir un groupe de journaux existant dans la même région que le suivi.

   > **Note**
   >
   > Un journal qui s'applique à toutes les régions envoie les fichiers journaux de toutes les régions au groupe de CloudWatch journaux journaux que vous spécifiez.

4. Dans CloudWatch Logs, sélectionnez Modifier.
5. Pour CloudWatch Logs, choisissez Enabled.
6. Dans Nom du groupe de journaux, choisissez Nouveau pour créer un nouveau groupe de journaux, ou Existant pour utiliser un groupe existant. Si vous choisissez Nouveau, vous CloudTrail spécifiez un nom pour le nouveau groupe de journaux ou vous pouvez saisir un nom. Pour plus d'informations sur la dénomination, veuillez consulter CloudWatch dénomination des groupes de journaux et des flux de journaux pour CloudTrail.
7. Si vous choisissez Existant, choisissez un groupe de journaux dans la liste déroulante.
8. Dans Nom du rôle, choisissez Nouveau pour créer un nouveau rôle IAM afin d'obtenir les autorisations d'envoyer des CloudWatch journaux à Logs. Choisir Existant pour choisir un rôle IAM existant dans la liste déroulante. L'instruction de politique pour le rôle nouveau ou existant s'affiche lorsque vous déroulez Document de politique. Pour plus d'informations sur ce rôle, consultez Document de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance.

> **Note**
>
> Lorsque vous configurez un journal de suivi, vous pouvez choisir un compartiment S3 et une rubrique SNS qui appartiennent à un autre compte. Toutefois, si vous souhaitez CloudTrail transmettre des événements à un groupe de CloudWatch journaux journaux, vous devez choisir un groupe de journaux existant dans votre compte actuel.

9. Sélectionnez Enregistrer les modifications.

Spécification d'un rôle IAM

Vous pouvez spécifier un rôle CloudTrail à assumer pour transmettre les événements au flux de log.

Pour spécifier un rôle

1. Par défaut, le `CloudTrail_CloudWatchLogs_Role` est spécifié pour vous. La politique de rôle par défaut dispose des autorisations requises pour créer un flux de CloudWatch journaux dans un groupe de journaux que vous spécifiez et pour transmettre des CloudTrail événements à ce flux de journaux.

   > **Note**
   >
   > Si vous souhaitez utiliser ce rôle pour un groupe de journaux d'un journal d'activité d'organisation, vous devez modifier manuellement la politique après la création du rôle. Pour plus d'informations, consultez cet exemple de politique et Création d'un journal de suivi pour une organisation.

   a. Pour vérifier le rôle, accédez à la AWS Identity and Access Management console à l'adresse https://console.aws.amazon.com/iam/.

   b. Choisissez Rôles, puis choisissez le CloudTrail_ CloudWatchLogs _Role.

   c. Dans l'onglet Autorisations, développez la politique pour afficher son contenu.

2. Vous pouvez spécifier un autre rôle, mais vous devez associer la politique de rôle requise au rôle existant si vous souhaitez l'utiliser pour envoyer des événements à CloudWatch Logs. Pour plus d'informations, consultez Document de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance.

Affichage des événements dans la CloudWatch console

Après avoir configuré votre journal pour envoyer des événements à votre groupe de CloudWatch journaux Logs, vous pouvez consulter les événements dans la CloudWatch console. CloudTrail transmet généralement les événements à votre groupe de log dans un délai moyen d'environ 5 minutes après un appel d'API. Ce délai n'est pas garanti. Pour plus d'informations, consultez le Contrat de niveau de service (SLA)AWS CloudTrail.

Pour afficher les événements dans la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation de gauche, sous Journaux, choisissez Groupes de journaux.
3. Choisissez le groupe de journaux que vous avez spécifié pour votre journal d'activité.
4. Choisissez le flux de journaux que vous souhaitez afficher.
5. Pour afficher les détails de l'événement consigné par votre journal d'activité, choisissez un événement.

> **Note**
>
> La colonne Heure (UTC) de la CloudWatch console indique la date à laquelle l'événement a été transmis à votre groupe de journaux. Pour connaître l'heure réelle à laquelle l'événement a été enregistré CloudTrail, consultez le `eventTime` champ.

Configuration de la surveillance des CloudWatch journaux avec le AWS CLI

Vous pouvez utiliser le AWS CLI pour configurer l'envoi CloudTrail d'événements aux CloudWatch journaux à des fins de surveillance.

Création d'un groupe de journaux

1. Si vous n'avez pas de groupe de CloudWatch journaux existant, créez-en un en tant que point de terminaison de diffusion pour les événements de journal à l'aide de la `create-log-group` commande CloudWatch Logs.

```
aws logs create-log-group --log-group-name name
```

L'exemple suivant crée un groupe de journaux nommé `CloudTrail/logs` :

```
aws logs create-log-group --log-group-name CloudTrail/logs
```

2. Récupérez l'Amazon Resource Name (ARN) du groupe de journaux.

```
aws logs describe-log-groups
```

Création d'un rôle

Créez un rôle lui CloudTrail permettant d'envoyer des événements au groupe de CloudWatch journaux Logs. La commande `create-role` IAM prend deux paramètres : un nom de rôle et un chemin d'accès vers un document de politique d'endossement de rôle au format JSON. Le document de politique que vous utilisez donne `AssumeRole` des autorisations à CloudTrail. La commande `create-role` crée le rôle avec les autorisations requises.

Pour créer le fichier JSON qui contiendra le document de politique, ouvrez un éditeur de texte et enregistrez le contenu de la politique suivante dans un fichier nommé `assume_role_policy_document.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Exécutez la commande suivante pour créer le rôle avec `AssumeRole` des autorisations pour CloudTrail.

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

Lorsque la commande est terminée, prenez note de l'ARN du rôle dans la sortie.

Création d'un document de politique

Créez le document de politique de rôle suivant pour CloudTrail. Ce document accorde CloudTrail les autorisations requises pour créer un flux de CloudWatch journaux dans le groupe de journaux que vous spécifiez et pour transmettre des CloudTrail événements à ce flux de journaux.

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

Enregistrez le document de politique dans un fichier nommé `role-policy-document.json`.

Si vous créez une politique qui peut être utilisée pour les journaux d'activité de l'organisation, vous devrez la configurer légèrement différemment. *Par exemple, la politique suivante accorde CloudTrail les autorisations requises pour créer un flux de*

journaux dans le groupe de CloudWatch journaux que vous spécifiez et pour transmettre des CloudTrail événements à ce flux de journaux, à la fois pour les traces du AWS compte 111111111111 et pour les pistes d'organisation créées dans le compte 111111111111 qui sont appliquées à l'organisation avec l'ID o-exampleorgid : AWS Organizations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Pour plus d'informations sur les journaux d'activité d'organisation, consultez Création d'un journal de suivi pour une organisation.

Exécutez la commande suivante pour appliquer la politique au rôle.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

Mise à jour du journal d'activité

Mettez à jour le journal avec les informations relatives au groupe de journaux et au rôle à l'aide de la CloudTrail `update-trail` commande.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

Pour plus d'informations sur les AWS CLI commandes, consultez la référence de ligne de AWS CloudTrail commande.

Limitation

CloudWatch Les journaux autorisent EventBridge chacun une taille d'événement maximale de 256 Ko. Bien que la taille maximale de la plupart des événements de service soit de 256 Ko, certains services comportent tout de même des événements plus importants. CloudTrail n'envoie pas ces événements à CloudWatch Logs ou EventBridge.

À CloudTrail partir de la version 1.05, la taille maximale des événements est de 256 Ko. Cela permet d'empêcher l'exploitation par des acteurs malveillants et de permettre à d'autres AWS services, tels que CloudWatch Logs et EventBridge.

Création d' CloudWatch alarmes pour CloudTrail des événements : exemples

Cette rubrique décrit comment configurer les alarmes pour les CloudTrail événements et inclut des exemples.

Rubriques

Prérequis

Pour pouvoir utiliser les exemples dans cette rubrique, vous devez :

- Créer un journal de suivi avec la console ou la CLI.
- Créez un groupe de journaux, ce que vous pouvez faire dans le cadre de la création d'un journal de suivi. Pour plus d'informations sur la création d'un journal de suivi, consultez Création d'un journal de suivi.
- Spécifiez ou créez un rôle IAM qui accorde CloudTrail les autorisations nécessaires pour créer un flux de CloudWatch journaux dans le groupe de journaux que vous spécifiez et pour transmettre des CloudTrail événements à ce flux de journaux. Le `CloudTrail_CloudWatchLogs_Role` par défaut s'en charge pour vous.

Pour plus d'informations, consultez Envoyer des événements à CloudWatch Logs. Les exemples présentés dans cette section sont exécutés dans la console Amazon CloudWatch Logs. Pour plus d'informations sur la création de filtres métriques et d'alarmes, consultez les sections Création de métriques à partir des événements du journal à l'aide de filtres et Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Créer un filtre de métrique et une alarme

Pour créer une alarme, vous devez d'abord créer un filtre de métrique, puis configurer une alarme basée sur le filtre. Les procédures sont affichées pour tous les exemples. Pour plus d'informations sur la syntaxe des filtres métriques et des modèles pour les événements de CloudTrail journal, consultez les sections relatives au JSON relatives à la syntaxe des filtres et des modèles dans le guide de l'utilisateur Amazon CloudWatch Logs.

Exemple : modifications apportées à la configuration du groupe de sécurité

Suivez cette procédure pour créer une CloudWatch alarme Amazon qui se déclenche lorsque des modifications de configuration sont apportées aux groupes de sécurité.

Créer un filtre de métrique

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation de gauche, choisissez Journaux, Groupes de journaux.
3. Dans la liste des groupes de journaux, sélectionnez le groupe de journaux que vous avez créé pour votre journal de suivi.

4. Dans le menu Filtres métriques ou Actions, sélectionnez Créer un filtre de métrique.
5. Dans la page Define pattern (Définir un modèle), dans Create filter pattern (Créer un modèle de filtre), saisissez ce qui suit pour Filter pattern (Modèle de filtre).

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. Dans Test pattern (Modèle de test), laissez les valeurs par défaut. Choisissez Next (Suivant).
7. Dans la page Attribuer une métrique, sous Nom de filtre, saisissez **`SecurityGroupEvents`**.
8. Dans Détails de la métrique, activez Créer un nouveau, puis saisissez **`CloudTrailMetrics`** pour Espace de noms de métrique.
9. Dans Nom de la métrique, saisissez **`SecurityGroupEventCount`**.
10. Dans Valeur de métriques, saisissez **`1`**.
11. Laissez la Valeur par défaut vide.
12. Choisissez Next Suivant.
13. Sur la page Review and create (Vérifier et créer), vérifiez vos choix. Choisissez Create metric filter (Créer un filtre de métriques) pour créer le filtre, ou choisissez Edit (Modifier) pour revenir en arrière et modifier les valeurs.

Créer une alarme

Une fois que vous avez créé le filtre métrique, la page des détails du groupe de CloudWatch journaux de votre groupe CloudTrail de journaux de suivi s'ouvre. Suivez cette procédure ci-dessous pour créer une alarme.

1. Dans la page Metric filters (Filtres de métriques), recherchez le filtre de mesure que vous avez créé dans the section called “Créer un filtre de métrique”. Remplissez la case pour le filtre de métrique. Dans Metric filters (Filtres de métriques), choisissez Create alarm (Créer une alarme).
2. Pour Spécifier la métrique et les conditions, saisissez ce qui suit.
   a. Pour Graph (Graphe), la ligne est définie sur **`1`** en fonction des autres paramètres que vous effectuez lorsque vous créez votre alarme.
   b. Pour Metric name (Nom de la métrique), conservez le nom de la métrique actuelle, **`SecurityGroupEventCount`**.

c. Pour Statistic (Statistique), conservez la valeur par défaut, **`Sum`**.

d. Pour Period (Période), conservez la valeur par défaut, **`5 minutes`**.

e. Dans la section Conditions sous Threshold type (Type de seuil), choisissez Static (Statique).

f. Pour Whenever ***`metric_name`*** (À chaque fois que le nom de la métrique) est, choisissez Greater/Equal (Supérieur/Égal).

g. Pour la valeur du seuil, saisissez **`1`**.

h. Dans Additional configuration (Configuration supplémentaire), laissez les valeurs par défaut. Choisissez Next (Suivant).

3. Sur la page Configurer les actions, choisissez Notification, puis sélectionnez En alarme, ce qui indique que l'action est entreprise lorsque le seuil d'un événement de changement en 5 minutes est dépassé et qu'elle SecurityGroupEventCountest en état d'alarme.

   a. Pour Envoyer une notification à la rubrique SNS suivante, choisissez Créer une rubrique.

   b. Saisissez **`SecurityGroupChanges_CloudWatch_Alarms_Topic`** comme nom de la nouvelle rubrique Amazon SNS.

   c. Dans Points de terminaison d'e-mail qui reçoivent la notification, saisissez les adresses e-mail des utilisateurs que vous souhaitez recevoir des notifications si cette alarme est déclenchée. Séparez les adresses e-mail par des virgules.

      Chaque destinataire d'un e-mail recevra un e-mail lui demandant de confirmer qu'il souhaite être abonné à la rubrique Amazon SNS.

   d. Choisissez Create topic (Créer une rubrique).

4. Dans cet exemple, ignorez les autres types d'action. Choisissez Next (Suivant).

5. Dans la page Add name and description (Ajouter le nom et la description), saisissez un nom convivial pour l'alarme et une description. Pour cet exemple, saisissez **`Security group configuration changes`** pour le nom, puis **`Raises alarms if security group configuration changes occur`** pour la description. Choisissez Next (Suivant).

6. Dans la page Preview and create (Prévisualiser et créer), vérifiez vos choix. Choisissez Edit (Modifier) pour effectuer des modifications, ou choisissez Create alarm (Créer une alarme) pour créer l'alarme.

   Après avoir créé l'alarme, CloudWatch ouvre la page Alarmes. La colonne Actions de l'alarme indique Pending confirmation (En attente de confirmation) jusqu'à ce que tous les destinataires d'e-mails de la rubrique SNS aient confirmé qu'ils souhaitent s'abonner aux notifications SNS.

Exemples d' AWS Management Console échecs de connexion

Suivez cette procédure pour créer une CloudWatch alarme Amazon qui se déclenche en cas d'échec de AWS Management Console connexion au moins trois fois sur une période de cinq minutes.

Créer un filtre de métrique

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation de gauche, choisissez Journaux, Groupes de journaux.
3. Dans la liste des groupes de journaux, sélectionnez le groupe de journaux que vous avez créé pour votre journal de suivi.
4. Dans le menu Filtres métriques ou Actions, sélectionnez Créer un filtre de métrique.
5. Dans la page Define pattern (Définir un modèle), dans Create filter pattern (Créer un modèle de filtre), saisissez ce qui suit pour Filter pattern (Modèle de filtre).

   ```
   { ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
   ```

6. Dans Test pattern (Modèle de test), laissez les valeurs par défaut. Choisissez Next (Suivant).
7. Dans la page Attribuer une métrique, sous Nom de filtre, saisissez **`ConsoleSignInFailures`**.
8. Dans Détails de la métrique, activez Créer un nouveau, puis saisissez **`CloudTrailMetrics`** pour Espace de noms de métrique.
9. Dans Nom de la métrique, saisissez **`ConsoleSigninFailureCount`**.
10. Dans Valeur de métriques, saisissez **`1`**.
11. Laissez la Valeur par défaut vide.
12. Choisissez Next Suivant.
13. Sur la page Review and create (Vérifier et créer), vérifiez vos choix. Choisissez Create metric filter (Créer un filtre de métriques) pour créer le filtre, ou choisissez Edit (Modifier) pour revenir en arrière et modifier les valeurs.

Créer une alarme

Une fois que vous avez créé le filtre métrique, la page des détails du groupe de CloudWatch journaux de votre groupe CloudTrail de journaux de suivi s'ouvre. Suivez cette procédure ci-dessous pour créer une alarme.

1. Dans la page Metric filters (Filtres de métriques), recherchez le filtre de mesure que vous avez créé dans the section called "Créer un filtre de métrique". Remplissez la case pour le filtre de métrique. Dans Metric filters (Filtres de métriques), choisissez Create alarm (Créer une alarme).
2. Dans la page Create alarm (Créer une alarme), dans Specify metric and conditions (Spécifier la métrique et les conditions), saisissez ce qui suit.

   a. Pour Graph (Graphe), la ligne est définie sur **3** en fonction des autres paramètres que vous effectuez lorsque vous créez votre alarme.

   b. Pour Metric name (Nom de la métrique), conservez le nom de la métrique actuelle, **ConsoleSigninFailureCount**.

   c. Pour Statistic (Statistique), conservez la valeur par défaut, **Sum**.

   d. Pour Period (Période), conservez la valeur par défaut, **5 minutes**.

   e. Dans la section Conditions sous Threshold type (Type de seuil), choisissez Static (Statique).

   f. Pour Whenever ***metric_name*** (À chaque fois que le nom de la métrique) est, choisissez Greater/Equal (Supérieur/Égal).

   g. Pour la valeur du seuil, saisissez **3**.

   h. Dans Additional configuration (Configuration supplémentaire), laissez les valeurs par défaut. Choisissez Next (Suivant).
3. Sur la page Configurer les actions, pour Notification, choisissez En alarme, ce qui indique que l'action est entreprise lorsque le seuil de 3 événements de changement en 5 minutes est dépassé et qu'elle ConsoleSigninFailureCountest en état d'alarme.

   a. Pour Envoyer une notification à la rubrique SNS suivante, choisissez Créer une rubrique.

   b. Saisissez **ConsoleSignInFailures_CloudWatch_Alarms_Topic** comme nom de la nouvelle rubrique Amazon SNS.

   c. Dans Points de terminaison d'e-mail qui reçoivent la notification, saisissez les adresses e-mail des utilisateurs que vous souhaitez recevoir des notifications si cette alarme est déclenchée. Séparez les adresses e-mail par des virgules.

      Chaque destinataire d'un e-mail recevra un e-mail lui demandant de confirmer qu'il souhaite être abonné à la rubrique Amazon SNS.

   d. Choisissez Create topic (Créer une rubrique).
4. Dans cet exemple, ignorez les autres types d'action. Choisissez Next (Suivant).
5. Dans la page Add name and description (Ajouter le nom et la description), saisissez un nom convivial pour l'alarme et une description. Pour cet exemple, saisissez **Console sign-in**

failures pour le nom, puis **Raises alarms if more than 3 console sign-in failures occur in 5 minutes** pour la description. Choisissez Next (Suivant).

6. Dans la page Preview and create (Prévisualiser et créer), vérifiez vos choix. Choisissez Edit (Modifier) pour effectuer des modifications, ou choisissez Create alarm (Créer une alarme) pour créer l'alarme.

   Après avoir créé l'alarme, CloudWatch ouvre la page Alarmes. La colonne Actions de l'alarme indique Pending confirmation (En attente de confirmation) jusqu'à ce que tous les destinataires d'e-mails de la rubrique SNS aient confirmé qu'ils souhaitent s'abonner aux notifications SNS.

Exemple : modifications apportées à une stratégie &IAM;

Suivez cette procédure pour créer une CloudWatch alarme Amazon qui est déclenchée lorsqu'un appel d'API est effectué pour modifier une politique IAM.

Créer un filtre de métrique

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Logs (Journaux).
3. Dans la liste des groupes de journaux, sélectionnez le groupe de journaux que vous avez créé pour votre journal de suivi.
4. Choisissez Actions, puis Create metric filter (Créer un filtre de métrique).
5. Dans la page Define pattern (Définir un modèle), dans Create filter pattern (Créer un modèle de filtre), saisissez ce qui suit pour Filter pattern (Modèle de filtre).

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. Dans Test pattern (Modèle de test), laissez les valeurs par défaut. Choisissez Next (Suivant).
7. Dans la page Attribuer une métrique, sous Nom de filtre, saisissez **IAMPolicyChanges**.
8. Dans Détails de la métrique, activez Créer un nouveau, puis saisissez **CloudTrailMetrics** pour Espace de noms de métrique.

9. Dans Nom de la métrique, saisissez **`IAMPolicyEventCount`**.
10. Dans Valeur de métriques, saisissez **`1`**.
11. Laissez la Valeur par défaut vide.
12. Choisissez Next Suivant.
13. Sur la page Review and create (Vérifier et créer), vérifiez vos choix. Choisissez Create metric filter (Créer un filtre de métriques) pour créer le filtre, ou choisissez Edit (Modifier) pour revenir en arrière et modifier les valeurs.

Créer une alarme

Une fois que vous avez créé le filtre métrique, la page des détails du groupe de CloudWatch journaux de votre groupe CloudTrail de journaux de suivi s'ouvre. Suivez cette procédure ci-dessous pour créer une alarme.

1. Dans la page Metric filters (Filtres de métriques), recherchez le filtre de mesure que vous avez créé dans the section called “Créer un filtre de métrique”. Remplissez la case pour le filtre de métrique. Dans Metric filters (Filtres de métriques), choisissez Create alarm (Créer une alarme).
2. Dans la page Create alarm (Créer une alarme), dans Specify metric and conditions (Spécifier la métrique et les conditions), saisissez ce qui suit.

   a. Pour Graph (Graphe), la ligne est définie sur **`1`** en fonction des autres paramètres que vous effectuez lorsque vous créez votre alarme.

   b. Pour Metric name (Nom de la métrique), conservez le nom de la métrique actuelle, **`IAMPolicyEventCount`**.

   c. Pour Statistic (Statistique), conservez la valeur par défaut, **`Sum`**.

   d. Pour Period (Période), conservez la valeur par défaut, **`5 minutes`**.

   e. Dans la section Conditions sous Threshold type (Type de seuil), choisissez Static (Statique).

   f. Pour Whenever ***`metric_name`*** (À chaque fois que le nom de la métrique) est, choisissez Greater/Equal (Supérieur/Égal).

   g. Pour la valeur du seuil, saisissez **`1`**.

   h. Dans Additional configuration (Configuration supplémentaire), laissez les valeurs par défaut. Choisissez Next (Suivant).

   i.

3. Sur la page Configurer les actions, pour Notification, choisissez En alarme, ce qui indique que l'action est entreprise lorsque le seuil d'un événement de changement en 5 minutes est dépassé et que IAM PolicyEventCount est en état d'alarme.

   a. Pour Envoyer une notification à la rubrique SNS suivante, choisissez Créer une rubrique.

   b. Saisissez **`IAM_Policy_Changes_CloudWatch_Alarms_Topic`** comme nom de la nouvelle rubrique Amazon SNS.

   c. Dans Points de terminaison d'e-mail qui reçoivent la notification, saisissez les adresses e-mail des utilisateurs que vous souhaitez recevoir des notifications si cette alarme est déclenchée. Séparez les adresses e-mail par des virgules.

      Chaque destinataire d'un e-mail recevra un e-mail lui demandant de confirmer qu'il souhaite être abonné à la rubrique Amazon SNS.

   d. Choisissez Create topic (Créer une rubrique).

4. Dans cet exemple, ignorez les autres types d'action. Choisissez Next (Suivant).

5. Dans la page Add name and description (Ajouter le nom et la description), saisissez un nom convivial pour l'alarme et une description. Pour cet exemple, saisissez **`IAM Policy Changes`** pour le nom, puis **`Raises alarms if IAM policy changes occur`** pour la description. Choisissez Next (Suivant).

6. Dans la page Preview and create (Prévisualiser et créer), vérifiez vos choix. Choisissez Edit (Modifier) pour effectuer des modifications, ou choisissez Create alarm (Créer une alarme) pour créer l'alarme.

   Après avoir créé l'alarme, CloudWatch ouvre la page Alarmes. La colonne Actions de l'alarme indique Pending confirmation (En attente de confirmation) jusqu'à ce que tous les destinataires d'e-mails de la rubrique SNS aient confirmé qu'ils souhaitent s'abonner aux notifications SNS.

Configuration des notifications pour les alarmes CloudWatch Logs

Vous pouvez configurer CloudWatch Logs pour envoyer une notification chaque fois qu'une alarme est déclenchée CloudTrail. Cela vous permet de réagir rapidement aux événements opérationnels critiques enregistrés dans les CloudTrail événements et détectés par CloudWatch les journaux. CloudWatch utilise Amazon Simple Notification Service (SNS) pour envoyer des e-mails. Pour plus d'informations, consultez la section Configuration des notifications Amazon SNS dans le guide de l'CloudWatch utilisateur.

Arrêter CloudTrail d'envoyer des événements à CloudWatch Logs

Vous pouvez arrêter d'envoyer AWS CloudTrail des événements à Amazon CloudWatch Logs en mettant à jour un journal pour désactiver les paramètres CloudWatch des journaux.

Arrêter d'envoyer des événements à CloudWatch Logs (console)

Pour arrêter d'envoyer CloudTrail des événements à CloudWatch Logs

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation, choisissez Journaux de suivi.
3. Choisissez le nom de la piste pour laquelle vous souhaitez désactiver l'intégration CloudWatch des journaux.
4. Dans CloudWatch Logs, sélectionnez Modifier.
5. Désactivez la case à cocher Activé.
6. Sélectionnez Enregistrer les modifications.

Arrêter d'envoyer des événements à CloudWatch Logs (CLI)

Vous pouvez supprimer le groupe de CloudWatch journaux Logs en tant que point de terminaison de livraison en exécutant la update-trailcommande. La commande suivante efface le groupe de journaux et le rôle de la configuration de suivi en remplaçant les valeurs de l'ARN du groupe de CloudWatch journaux et de l'ARN du rôle des journaux par des valeurs vides.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch dénomination des groupes de journaux et des flux de journaux pour CloudTrail

Amazon CloudWatch affichera le groupe de journaux que vous avez créé pour les CloudTrail événements aux côtés de tous les autres groupes de journaux que vous avez dans une région. Nous recommandons d'utiliser un nom de groupe de journaux qui permet de distinguer facilement le groupe de journaux d'autres. Par exemple, **`CloudTrail/logs`**.

Suivez ces instructions ci-dessous pour nommer un groupe de journaux :

- Les noms de groupes de journaux doivent être uniques dans la région d'un Compte AWS.
- Les noms des groupes de journaux peuvent comporter entre 1 et 512 caractères.
- Les noms de groupes de journaux contiennent les caractères suivants : a-z, A-Z, 0-9, « _ » (trait de soulignement), « - » (tiret), '/' (barre oblique) et « . » (point).

Lors de CloudTrail la création du flux de journaux pour le groupe de journaux, il nomme le flux de journaux selon le format suivant : Account_ID _ CloudTrail _ trail_region.

> **Note**
>
> Si le volume de CloudTrail journaux est important, plusieurs flux de journaux peuvent être créés pour fournir des données de journal à votre groupe de journaux. *Lorsqu'il existe plusieurs flux de journaux, CloudTrail nommez chaque flux de journal selon le format suivant : Account_ID _ _ CloudTrail trail_region _ number.*

Pour plus d'informations sur les groupes de CloudWatch journaux, consultez la section Utilisation des groupes de journaux et des flux de CloudWatch journaux dans le guide de l'utilisateur Amazon Logs et CreateLogGroupdans le manuel Amazon CloudWatch Logs API Reference.

Document de politique de rôle pour l'utilisation CloudTrail des CloudWatch journaux à des fins de surveillance

Cette section décrit la politique d'autorisation requise pour que le CloudTrail rôle envoie des événements de journal à CloudWatch Logs. Vous pouvez joindre un document de politique à un rôle lorsque vous configurez CloudTrail pour envoyer des événements, comme décrit dansEnvoyer des événements à CloudWatch Logs. Vous pouvez également créer un rôle à l'aide d'IAM. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un rôle Service AWS ou Création d'un rôle IAM (AWS CLI).

L'exemple de document de politique suivant contient les autorisations requises pour créer un flux de CloudWatch journaux dans le groupe de journaux que vous spécifiez et pour transmettre CloudTrail des événements à ce flux de journaux dans la région USA Est (Ohio). (C'est la politique par défaut pour le rôle IAM par défaut `CloudTrail_CloudWatchLogs_Role`.)

> **Note**
>
> La prévention de la confusion chez les adjoints ne s'applique pas à la politique des rôles pour la surveillance des CloudWatch journaux. La politique des rôles ne prend pas en charge l'utilisation de `aws:SourceArn` et`aws:SourceAccount`.

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

Si vous créez une politique qui peut être utilisée aussi pour les journaux d'activité d'organisation, vous devez la modifier à partir de la politique par défaut créée pour le rôle. *Par exemple, la politique suivante accorde CloudTrail les autorisations requises pour créer un flux de journaux dans le groupe de CloudWatch journaux que*

vous spécifiez comme valeur de log_group_name, et pour transmettre des CloudTrail événements à ce flux de journal pour les traces du compte 111111111111 et pour les pistes d'organisation créées dans le AWS compte 111111111111 qui sont appliquées à l'organisation avec l'ID o-exampleorgid : AWS Organizations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Pour plus d'informations sur les journaux d'activité d'organisation, consultez Création d'un journal de suivi pour une organisation.

Réception de fichiers CloudTrail journaux provenant de plusieurs comptes

Vous pouvez CloudTrail envoyer des fichiers journaux à partir de plusieurs Comptes AWS dans un seul compartiment Amazon S3. Par exemple, vous en avez quatre Comptes AWS avec les ID de compte 1111111111, 222222222222, 333333333333 et 444444444444, et vous souhaitez configurer pour transmettre les fichiers journaux de ces quatre comptes à un compartiment appartenant au compte 111111111111. CloudTrail Pour ce faire, suivez scrupuleusement les étapes suivantes:

1. Créez un journal de suivi dans le compte auquel le compartiment de destination appartient (111111111111, en l'occurrence). Ne créez pas encore de journal de suivi pour d'autres comptes.

   Pour obtenir des instructions, veuillez consulter Créer un journal de suivi dans la console.

2. Mettez à jour la politique de compartiment de votre compartiment de destination pour accorder des autorisations entre comptes à CloudTrail.

   Pour obtenir des instructions, veuillez consulter Configuration de la politique de compartiment pour plusieurs comptes.

3. Créez un journal de suivi dans les autres comptes (222222222222, 333333333333 et 444444444444, en l'occurrence) pour lesquels vous souhaitez enregistrer des activités. Lorsque vous créez le journal de suivi dans chaque compte, indiquez le compartiment Amazon S3 appartenant au compte que vous avez spécifié à l'étape 1 (111111111111, en l'occurrence). Pour obtenir des instructions, veuillez consulter Créer des journaux de suivi dans des comptes supplémentaires.

   > **Note**
   >
   > Si vous choisissez d'activer le chiffrement SSE-KMS, la politique de clé KMS doit autoriser CloudTrail l'utilisation de la clé pour chiffrer vos fichiers journaux et autoriser les utilisateurs que vous spécifiez à lire les fichiers journaux sous forme non chiffrée. Pour en savoir plus sur la modification manuelle de la politique de clés, consultez Configurer les politiques AWS KMS clés pour CloudTrail.

Traitement des ID de compte de propriétaire du compartiment pour les événements de données appelés par d'autres comptes

Historiquement, si CloudTrail les événements de données étaient activés dans l'API Compte AWS d'un événement de données Amazon S3, l'ID de compte du propriétaire du compartiment S3 CloudTrail était affiché dans l'événement de données (tel que`PutObject`). Cela s'est produit même si les événements de données S3 n'étaient pas activés sur le compte propriétaire du compartiment.

CloudTrail Supprime maintenant l'ID de compte du propriétaire du compartiment S3 dans le `resources` bloc si les deux conditions suivantes sont remplies :

- L'appel d'API de l'événement de données provient d'un autre propriétaire Compte AWS que le propriétaire du compartiment Amazon S3.
- L'appelant de l'API a reçu une `AccessDenied` erreur qui concernait uniquement le compte appelant.

Le propriétaire de la ressource sur laquelle l'appel d'API a été effectué reçoit toujours l'événement complet.

Les extraits de registre d'événements suivants sont un exemple du comportement attendu. Dans l’extrait `Historic`, l'ID de compte 123456789012 du propriétaire du compartiment S3 est affiché à un appelant d'API à partir d'un autre compte. Dans l'exemple de comportement actuel, l'ID de compte du propriétaire du compartiment n'est pas affiché.

```
# Historic

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

Voici le comportement actuel.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

Rubriques

Configuration de la politique de compartiment pour plusieurs comptes

Pour qu'un compartiment puisse recevoir des fichiers journaux provenant de plusieurs comptes, sa politique de compartiment doit CloudTrail autoriser l'écriture de fichiers journaux à partir de tous les comptes que vous spécifiez. Cela signifie que vous devez modifier la politique de compartiment de votre compartiment de destination pour CloudTrail autoriser l'écriture de fichiers journaux à partir de chaque compte spécifié.

> **Note**
>
> Pour des raisons de sécurité, les utilisateurs non autorisés ne peuvent pas créer de journal de suivis incluant `AWSLogs/` en tant que `S3KeyPrefix` paramètre.

Pour modifier les autorisations de compartiment de sorte que les fichiers puissent être reçus à partir de plusieurs comptes

1. Connectez-vous à l' AWS Management Console aide du compte propriétaire du compartiment (111111111111 dans cet exemple) et ouvrez la console Amazon S3.

2. Choisissez le compartiment dans lequel CloudTrail vos fichiers journaux sont envoyés, puis sélectionnez Permissions.
3. Sous Bucket policy (Politique de compartiment), choisissez Edit (Modifier).
4. Modifiez la politique existante afin d'ajouter une ligne correspondant pour chaque compte supplémentaire dont vous voulez que les fichiers journaux soient livrés à ce compartiment. Examinez l'exemple de politique suivant, en particulier la ligne `Resource` soulignée qui spécifie un deuxième ID de compte. Comme bonne pratique en matière de sécurité, ajoutez une `aws:SourceArn` clé de condition de la politique de compartiment Amazon S3. Cela permet d'éviter tout accès non autorisé à votre compartiment S3. Si vous avez déjà des journaux d'activités, veillez à ajouter une ou plusieurs clés de condition.

> **Note**
>
> Un identifiant de AWS compte est un nombre à douze chiffres, y compris des zéros en tête.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
              "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
            ]
          }
       }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ],
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Créer des journaux de suivi dans des comptes supplémentaires

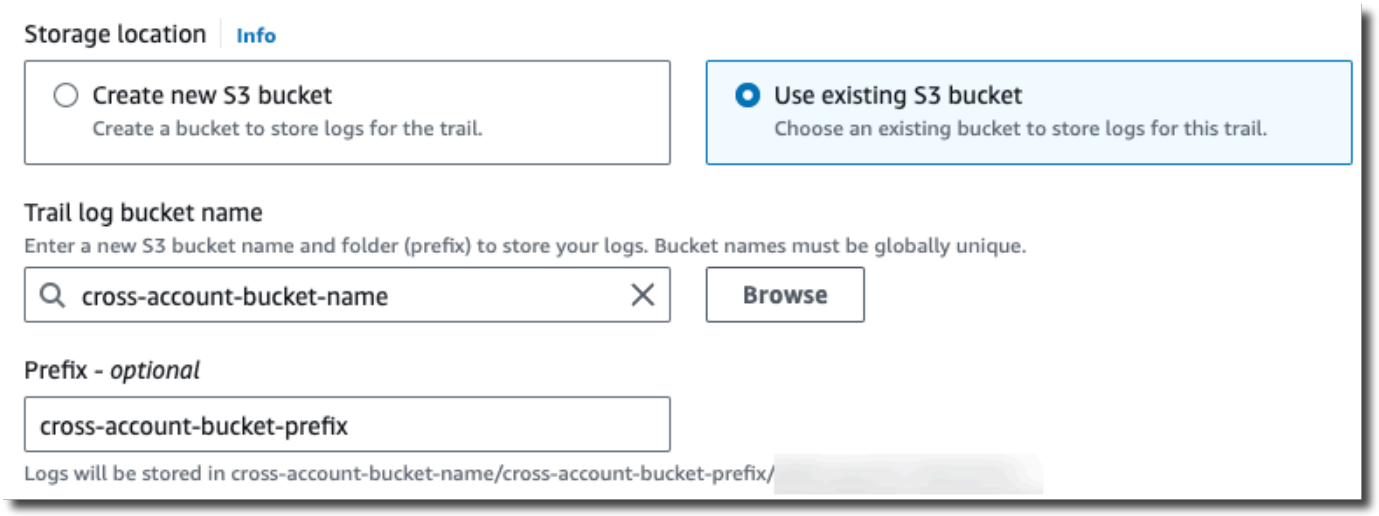
Vous pouvez utiliser la console ou le AWS CLI pour créer des traces supplémentaires Comptes AWS et agréger leurs fichiers journaux dans un compartiment Amazon S3. Vous pouvez également créer un journal d'organisation pour enregistrer tous Comptes AWS les membres d'une organisation AWS Organizations. Pour plus d'informations, consultez Création d'un journal de suivi pour une organisation.

Utiliser la console pour créer des parcours dans des AWS comptes supplémentaires

Vous pouvez utiliser la CloudTrail console pour créer des parcours dans des comptes supplémentaires.

1. Connectez-vous à l' AWS Management Console aide du compte pour lequel vous souhaitez créer un parcours. Suivez les étapes présentées dans Créer un journal de suivi dans la console pour créer un journal de suivi à l'aide de la console.
2. Pour Emplacement de stockage, choisissez Utiliser un compartiment S3 existant. Utilisez la zone de texte pour saisir le nom du compartiment que vous utilisez pour stocker les fichiers journaux des différents comptes.

> **Note**
>
> La politique du compartiment doit accorder CloudTrail l'autorisation d'y écrire. Pour en savoir plus sur la modification manuelle de la politique de compartiment, consultez Configuration de la politique de compartiment pour plusieurs comptes.



3. Dans Préfixe, saisissez le préfixe que vous utilisez pour stocker les fichiers journaux des différents comptes. Si vous choisissez d'utiliser un préfixe différent de celui que vous avez spécifié dans votre politique de compartiment, vous devez modifier la politique de compartiment de votre compartiment de destination pour autoriser CloudTrail l'écriture de fichiers journaux dans votre compartiment à l'aide de ce nouveau préfixe.

Utilisation de la CLI pour créer une trace dans des AWS comptes supplémentaires

Vous pouvez utiliser les outils de ligne de AWS commande pour créer des traces dans des comptes supplémentaires et agréger leurs fichiers journaux dans un compartiment Amazon S3. Pour plus d'informations sur ces outils, consultez cloudtrail dans le manuel AWS CLI Command Reference.

Créez un journal de suivi à l'aide de la commande create-trail, en spécifiant les attributs suivants :

- `--name` spécifie le nom du journal de suivi.
- `--s3-bucket-name` spécifie le compartiment Amazon S3 que vous utilisez pour stocker les fichiers journaux des différents comptes.
- `--s3-prefix` spécifie un préfixe pour le chemin de livraison du fichier journal (facultatif).

- `--is-multi-region-trail`indique que ce journal enregistrera les événements dans toutes les AWS régions de la partition dans laquelle vous travaillez.

Vous pouvez créer un parcours pour chaque région dans laquelle un compte gère AWS des ressources.

L'exemple de commande suivant indique comment créer un journal de suivis pour vos comptes supplémentaires à l'aide de l' AWS CLI. Pour que les fichiers journaux pour ces comptes soient livrés dans le compartiment que vous avez créé dans votre premier compte (111111111111, en l'occurrence), veuillez spécifier le nom du compartiment dans `--s3-bucket-name` l'option. Les noms de compartiment Amazon S3 sont généralement uniques.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail
```

Au moment de l'exécution de la commande, vous obtenez un résultat similaire à celui qui suit:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

Pour plus d'informations sur l'utilisation CloudTrail des outils de ligne de AWS commande, consultez la référence de la ligne de CloudTrail commande.

Partage de fichiers CloudTrail journaux entre AWS comptes

Cette section explique comment partager des fichiers CloudTrail journaux entre plusieurs AWS comptes. L'approche que vous utilisez pour partager les journaux entre Comptes AWS eux dépend de la configuration de votre compartiment S3. Les options de partage des fichiers journaux sont les suivantes :

- Propriétaire du compartiment imposé : la propriété d'objets S3 est un paramètre Amazon S3 au niveau des compartiments que vous pouvez utiliser pour contrôler la propriété des objets

qui sont chargés dans votre compartiment, ainsi que pour désactiver ou activer les listes de contrôle d'accès (ACL). Par défaut, la propriété d'objets est définie sur le paramètre Propriétaire du compartiment imposé, et toutes les listes ACL sont désactivées. Lorsque les listes ACL sont désactivées, le propriétaire du compartiment détient tous les objets présents dans le compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès. Lorsque l'option Propriétaire du compartiment imposé est définie, l'accès est géré par le biais de la politique du compartiment, ce qui évite aux utilisateurs d'avoir à assumer un rôle.

- Assumez un rôle pour partager des fichiers journaux : si vous n'avez pas choisi le paramètre Propriétaire du compartiment imposé, les utilisateurs devront assumer un rôle pour accéder aux fichiers journaux de votre compartiment S3.

Partager des fichiers journaux entre les comptes en assumant un rôle

> **Note**
>
> Cette section s'applique uniquement aux compartiments Amazon S3 qui n'utilisent pas le paramètre Propriétaire du compartiment imposé.

Cette section explique comment partager des fichiers CloudTrail journaux entre plusieurs personnes Comptes AWS en assumant un rôle et décrit les scénarios de partage de fichiers journaux.

- Scénario 1 : accordez l'accès en lecture seule aux comptes qui ont généré les fichiers journaux qui ont été placés dans votre compartiment Amazon S3.
- Scénario 2 : accordez l'accès à tous les fichiers journaux de votre compartiment Amazon S3 à un compte tiers qui peut analyser les fichiers journaux pour vous.

Pour accorder un accès en lecture seule aux fichiers journaux dans votre compartiment Amazon S3

1. Créez un rôle IAM pour chaque compte avec lequel vous souhaitez partager les fichiers journaux. Vous devez être administrateur pour accorder une autorisation.

   Lorsque vous créez le rôle, procédez comme suit :

   - Choisissez l'option Un autre Compte AWS.
   - Entrez l'ID de compte à 12 chiffres du compte devant bénéficier d'un accès.

- Cochez la case MFA requis si vous souhaitez que l'utilisateur fournissent une authentification multi-facteurs avant d'assumer le rôle.
- Choisissez la politique Amazon S3 ReadOnlyAccess.

> **Note**
>
> Par défaut, la ReadOnlyAccess politique Amazon S3 accorde des droits de récupération et de liste à tous les compartiments Amazon S3 de votre compte.

Pour plus de détails sur la gestion des autorisations pour les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

2. Créez une stratégie d'accès qui accorde l'accès en lecture seule au compte avec lequel vous voulez partager les fichiers journaux.
3. Demandez à chaque compte d'assumer un rôle pour récupérer des fichiers journaux.

Pour accorder un accès en lecture seule aux fichiers journaux avec un compte tiers

1. Créez un rôle IAM pour chaque compte tiers avec lequel vous souhaitez partager les fichiers journaux. Vous devez être administrateur pour accorder une autorisation.

   Lorsque vous créez le rôle, procédez comme suit :

   - Choisissez l'option Un autre Compte AWS.
   - Entrez l'ID de compte à 12 chiffres du compte devant bénéficier d'un accès.
   - Entrez un ID externe qui fournit un contrôle supplémentaire concernant les personnes pouvant assumer le rôle. Pour plus d'informations, consultez la section Comment utiliser un identifiant externe pour accorder l'accès à vos AWS ressources à un tiers dans le guide de l'utilisateur IAM.
   - Choisissez la politique Amazon S3 ReadOnlyAccess.

   > **Note**
   >
   > Par défaut, la ReadOnlyAccess politique Amazon S3 accorde des droits de récupération et de liste à tous les compartiments Amazon S3 de votre compte.

2. Créez une stratégie d'accès qui accorde l'accès en lecture seule au compte tiers avec lequel vous voulez partager les fichiers journaux.
3. Demandez au compte tiers d'assumer un rôle pour récupérer des fichiers journaux.

Les sections suivantes fournissent plus de détails sur ces étapes.

Rubriques

- Création d'une stratégie d'accès pour accorder l'accès aux comptes que vous détenez
- Création d'une stratégie d'accès pour accorder l'accès à un tiers
- Endossement d'un rôle
- Arrêtez de partager les fichiers CloudTrail journaux entre les AWS comptes

Création d'une stratégie d'accès pour accorder l'accès aux comptes que vous détenez

En tant que propriétaire du compartiment Amazon S3, vous avez le contrôle total du compartiment Amazon S3 dans lequel CloudTrail sont écrits les fichiers journaux des autres comptes. Vous souhaitez partager les fichiers journaux de chaque unité commerciale avec l'unité commerciale qui les a créés. Cependant, vous ne voulez pas qu'une unité puisse lire les fichiers journaux de n'importe quelle autre unité.

Par exemple, pour partager les fichiers journaux du compte B avec le compte B, mais pas avec le compte C, vous devez créer un nouveau rôle IAM dans votre compte qui spécifie que le compte B est un compte approuvé. Cette stratégie d'approbation de rôle spécifie que le compte B est approuvé pour assumer le rôle créé par votre compte ; elle doit ressembler à l'exemple suivant. La stratégie d'approbation est créée automatiquement si vous créez le rôle à l'aide de la console. Si vous utilisez le kit SDK pour créer le rôle, vous devez fournir la stratégie d'approbation en tant que paramètre de l'API `CreateRole`. Si vous utilisez la CLI pour créer le rôle, vous devez spécifier la stratégie d'approbation dans la commande de CLI `create-role`.

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

```
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Vous devez également créer une stratégie d'accès pour spécifier que le compte B peut lire uniquement l'emplacement dans lequel B a écrit ses fichiers journaux. La stratégie d'accès ressemblera à ce qui suit. Notez que l'ARN de la ressource inclut l'identifiant de compte à douze chiffres du compte B et le préfixe que vous avez spécifié, le cas échéant, lorsque vous avez activé le CloudTrail compte B pendant le processus d'agrégation. Pour plus d'informations sur la spécification d'un préfixe, consultez la page Créer des journaux de suivi dans des comptes supplémentaires.

> **Important**
>
> Vous devez vous assurer que le préfixe de la politique d'accès est exactement le même que celui que vous avez spécifié lorsque vous avez activé le compte B. Dans le cas contraire CloudTrail , vous devez modifier la politique d'accès aux rôles IAM de votre compte afin d'intégrer le préfixe réel du compte B. Si le préfixe de la politique d'accès aux rôles n'est pas exactement le même que celui que vous avez spécifié lorsque vous avez activé le compte B, le compte B ne pourra pas accéder CloudTrail à son journal fichiers.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
```

```
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

Utilisez la procédure précédente pour les éventuels comptes supplémentaires.

Après avoir créé des rôles pour chaque compte et spécifié les stratégies d'approbation et d'accès appropriées, et qu'un utilisateur IAM de chaque compte s'est vu attribuer des droits d'accès par l'administrateur de ce compte, un utilisateur IAM des comptes B ou C peut assumer le rôle par programmation.

Pour plus d'informations, consultez Endossement d'un rôle.

Création d'une stratégie d'accès pour accorder l'accès à un tiers

Vous devez créer un rôle IAM distinct pour un compte tiers. Lorsque vous créez le rôle, AWS créée automatiquement la relation d'approbation, ce qui spécifie que le compte tiers sera approuvé pour assumer le rôle. La stratégie d'accès pour le rôle spécifie les actions que le compte peut réaliser. Pour plus d'informations sur la création de rôles, consultez la page Création d'un rôle IAM.

Par exemple, la relation de confiance créée par AWS indique que le compte tiers (le compte Z dans cet exemple) est approuvé pour assumer le rôle que vous avez créé. Voici un exemple de politique d'approbation :

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole"
    }]
}
```

Si vous avez spécifié un ID externe lorsque vous avez créé le rôle pour le compte tiers, votre stratégie d'accès contient un élément `Condition` ajouté qui teste l'ID unique affecté par le compte.

Le test est effectué lorsque le rôle est assumé. L'exemple de stratégie d'accès suivant comporte un élément `Condition`.

Pour plus d'informations, consultez la section Comment utiliser un identifiant externe pour accorder l'accès à vos AWS ressources à un tiers dans le guide de l'utilisateur IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-account-Z"}}
    }]
}
```

Vous devez également créer une stratégie d'accès pour que votre compte spécifie que le compte tiers peut lire tous les journaux du compartiment Amazon S3. La stratégie d'accès doit ressembler à l'exemple suivant. Le caractère générique (*) à la fin de la valeur `Resource` indique que le compte tiers peut accéder à n'importe quel fichier journal dans le compartiment S3 auquel l'accès lui a été accordé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
```

```
        }
    ]
}
```

Après avoir créé un rôle pour le compte tiers et précisé la relation d'approbation et la stratégie d'accès appropriées, un utilisateur IAM du compte tiers doit assumer le rôle par programmation pour pouvoir lire les fichiers journaux à partir du compartiment. Pour plus d'informations, consultez Endossement d'un rôle.

Endossement d'un rôle

Vous devez désigner un utilisateur IAM distinct pour endosser chaque rôle que vous créez dans chaque compte. Vous devez ensuite vous assurer que chaque utilisateur IAM dispose des autorisations appropriées.

Utilisateurs et rôles IAM

Une fois que vous avez créé les rôles et les politiques nécessaires, vous devez désigner un utilisateur IAM dans chacun des comptes avec lesquels vous souhaitez partager des fichiers. Chaque utilisateur IAM assume par programmation le rôle approprié pour accéder aux fichiers journaux. Lorsqu'un utilisateur assume un rôle, AWS renvoie des informations d'identification de sécurité temporaires à cet utilisateur. Il peut ensuite faire des demandes pour répertorier, récupérer, copier ou supprimer des fichiers journaux en fonction des autorisations accordées par la stratégie d'accès associée au rôle.

Pour obtenir plus d'informations sur les identités IAM, veuillez consulter la page Identités IAM (utilisateurs, groupes d'utilisateurs et rôles).

La principale différence est la stratégie d'accès que vous créez pour chaque rôle IAM dans chaque scénario.

- Dans le scénario 1, la stratégie d'accès limite chaque compte à la lecture de ses propres fichiers journaux. Pour plus d'informations, consultez Création d'une stratégie d'accès pour accorder l'accès aux comptes que vous détenez.
- Dans le scénario 2, la stratégie d'accès du compte tiers l'autorise à lire tous les fichiers journaux qui sont agrégés dans le compartiment Amazon S3. Pour plus d'informations, consultez Création d'une stratégie d'accès pour accorder l'accès à un tiers.

Création de politiques d'autorisations pour les utilisateurs IAM

Pour effectuer les actions autorisées par un rôle, l'utilisateur IAM doit être autorisé à appeler l' AWS STS `AssumeRole`API. Vous devez modifier la politique de chaque utilisateur pour lui accorder les autorisations appropriées. Pour ce faire, vous définissez un élément Ressource dans la politique que vous associez à l'utilisateur IAM. L'exemple suivant montre une politique pour un utilisateur IAM du compte qui autorise l'utilisateur à assumer un rôle nommé `Test` créé précédemment par le compte A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

Pour modifier une politique gérée par le client (console)

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Dans la liste des politiques, choisissez le nom de la politique à modifier. Vous pouvez utiliser la zone de recherche pour filtrer la liste des politiques.
4. Choisissez l'onglet Autorisations, puis Modifier.
5. Effectuez l'une des actions suivantes :

   - Choisissez l'option Visuel pour modifier votre politique sans comprendre la syntaxe JSON. Vous pouvez apporter des modifications au service, aux ressources d'actions ou à des conditions facultatives pour chaque bloc d'autorisation de votre politique. Vous pouvez également importer une politique pour ajouter des autorisations supplémentaires au bas de votre politique. Lorsque vous avez fini d'apporter des modifications, choisissez Suivant pour continuer.

- Choisissez l'option JSON pour modifier votre politique en tapant ou en collant du texte dans la zone de texte JSON. Vous pouvez également importer une politique pour ajouter des autorisations supplémentaires au bas de votre politique. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés durant la validation de la politique, puis choisissez Suivant.

> **Note**
>
> Vous pouvez basculer à tout moment entre les options des éditeurs visuel et JSON. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, IAM peut restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour de plus amples informations, consultez la page Restructuration de politique dans le Guide de l'utilisateur IAM.

6. Sur la page Vérifier et enregistrer, vérifiez les Autorisations définies dans cette politique, puis choisissez Enregistrer les modifications pour enregistrer votre travail.
7. Si la politique gérée dispose déjà du maximum de cinq versions, une boîte de dialogue s'affiche lorsque vous choisissez Enregistrer les modifications. Pour enregistrer votre nouvelle version, la version la plus ancienne de la politique est supprimée et remplacée par cette nouvelle version. Vous pouvez choisir de définir la nouvelle version en tant que version par défaut de la politique.

   Choisissez Enregistrer les modifications pour enregistrer votre nouvelle version de la politique.

Appel AssumeRole

Un utilisateur peut assumer un rôle en créant une application qui appelle l' AWS STS `AssumeRole`API et transmet le nom de session du rôle, le numéro de ressource Amazon (ARN) du rôle à assumer et un identifiant externe facultatif. Le nom de séance de rôle est défini par le compte qui a créé le rôle à assumer. L'ID externe, le cas échéant, est défini par le compte tiers et transmis au compte propriétaire pour qu'il soit inclus lors de la création d'un rôle. Pour plus d'informations, consultez la section Comment utiliser un identifiant externe pour accorder l'accès à vos AWS ressources à un tiers dans le guide de l'utilisateur IAM. Vous pouvez récupérer l'ARN du compte A en ouvrant la console IAM.

Pour rechercher la valeur de l'ARN du compte A avec la console IAM

1. Sélectionnez Roles

2. Choisissez le rôle que vous souhaitez examiner.
3. Recherchez ARN du rôle dans la section Résumé.

L' AssumeRole API renvoie des informations d'identification temporaires à utiliser pour accéder aux ressources du compte propriétaire. Dans cet exemple, les ressources auxquelles vous souhaitez accéder sont le compartiment Amazon S3 et les fichiers journaux que contient le compartiment. Les informations d'identification temporaires disposent des autorisations que vous avez définies dans la stratégie d'accès du rôle.

L'exemple suivant de Python (qui utilise AWS SDK for Python (Boto)) montre comment appeler `AssumeRole` et comment utiliser les informations d'identification de sécurité temporaires renvoyées pour afficher tous les compartiments Amazon S3 contrôlés par le compte A.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
```

```
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

Arrêtez de partager les fichiers CloudTrail journaux entre les AWS comptes

Pour arrêter de partager des fichiers journaux avec un autre utilisateur Compte AWS, supprimez le rôle que vous avez créé pour ce compte. Pour plus d'informations sur la suppression d'un rôle, consultez la page Suppression de rôles ou de profils d'instance.

Validation de l' CloudTrail intégrité du fichier journal

Pour déterminer si un fichier journal a été modifié, supprimé ou inchangé après sa CloudTrail livraison, vous pouvez utiliser la validation de l'intégrité du fichier CloudTrail journal. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection. Vous pouvez utiliser le AWS CLI pour valider les fichiers à l'endroit où ils CloudTrail ont été livrés.

Pourquoi l'utiliser ?

Les fichiers journaux validés s'avèrent utiles lors d'enquêtes de sécurité et légales. Par exemple, un fichier journal validé permet d'affirmer que le fichier journal en question n'a pas été modifié ou que les informations d'identification d'un utilisateur donné ont réalisé une activité API spécifique. Le processus de validation de l'intégrité des fichiers CloudTrail journaux vous permet également de

savoir si un fichier journal a été supprimé ou modifié, ou de confirmer qu'aucun fichier journal n'a été envoyé à votre compte pendant une période donnée.

Comment ça marche

Lorsque vous activez la validation de l'intégrité du fichier journal, il CloudTrail crée un hachage pour chaque fichier journal fourni. Chaque heure, il crée et diffuse CloudTrail également un fichier qui fait référence aux fichiers journaux de la dernière heure et contient un hachage de chacun d'entre eux. Ce fichier s'appelle un fichier condensé. CloudTrail signe chaque fichier condensé à l'aide de la clé privée d'une paire de clés publique et privée. Après la livraison, vous pouvez utiliser la clé publique pour valider le fichier condensé. CloudTrail utilise des paires de clés différentes pour chacune d'entre elles Région AWS.

Les fichiers de résumé sont envoyés dans le même compartiment Amazon S3 associé à votre trace que vos fichiers CloudTrail journaux. Si vos fichiers journaux proviennent de toutes les régions ou de plusieurs comptes dans un seul compartiment Amazon S3, les fichiers de synthèse de ces régions et comptes CloudTrail seront transférés dans le même compartiment.

Les fichiers de valeur de hachage sont placés dans un dossier distinct de celui des fichiers-journaux. Cette séparation des fichiers de valeur de hachage et des fichiers journaux permet de mettre en application des stratégies de sécurité granulaires et permet aux solutions de traitement de fichiers journaux existantes de continuer à fonctionner sans modification. Chaque fichier de valeur de hachage contient également la signature numérique du fichier de valeur de hachage précédent, le cas échéant. La signature du fichier de valeur de hachage actuel se trouve dans les propriétés de métadonnées de l'objet Amazon S3 du fichier de valeur de hachage. Pour plus d'informations sur le contenu du fichier de valeur de hachage, consultez la page CloudTrail structure du fichier digest.

Stockage des fichiers journaux et des fichiers de valeur de hachage

Vous pouvez stocker les fichiers CloudTrail journaux et les fichiers de synthèse dans Amazon S3 ou S3 Glacier de manière sécurisée, durable et économique pendant une durée indéterminée. Afin d'améliorer la sécurité des fichiers de valeur de hachage stockés dans Amazon S3, vous pouvez utiliser la fonction Amazon S3 MFA Delete (Amazon S3 Supprimer MFA).

Activer la validation et les fichiers de validation

Pour activer la validation de l'intégrité du fichier journal, vous pouvez utiliser l' AWS Management Console API AWS CLI, ou CloudTrail l'API. L'activation de la validation de l'intégrité CloudTrail des fichiers journaux permet de fournir des fichiers journaux de synthèse à votre compartiment Amazon

S3, mais ne valide pas l'intégrité des fichiers. Pour plus d'informations, consultez Activation de la validation de l'intégrité des fichiers journaux pour CloudTrail.

Pour valider l'intégrité des fichiers CloudTrail journaux, vous pouvez utiliser AWS CLI ou créer votre propre solution. Les fichiers AWS CLI seront validés à l'endroit où ils CloudTrail ont été livrés. Si vous souhaitez valider les journaux que vous avez déplacé vers un autre emplacement, dans Amazon S3 ou ailleurs, vous pouvez créer vos propres outils de validation.

Pour plus d'informations sur la validation des journaux à l'aide du AWS CLI, consultezValidation de l'intégrité du fichier CloudTrail journal à l'aide du AWS CLI. Pour plus d'informations sur le développement d'implémentations personnalisées de la validation des fichiers CloudTrail journaux, consultezImplémentations personnalisées de validation de l'intégrité des fichiers CloudTrail journaux.

Activation de la validation de l'intégrité des fichiers journaux pour CloudTrail

Vous pouvez activer la validation de l'intégrité des fichiers journaux à l' AWS Management Console aide de l'interface de ligne de AWS commande (AWS CLI) ou de CloudTrail l'API. CloudTrail commence à livrer les fichiers de résumé dans environ une heure.

AWS Management Console

Pour activer la validation de l'intégrité du fichier journal avec la CloudTrail console, choisissez Oui pour l'option Activer la validation du fichier journal lorsque vous créez ou mettez à jour un journal. Par défaut, cette fonctionnalité est activée pour les nouveaux suivis. Pour plus d'informations, consultez Création et mise à jour d'un journal d'activité à l'aide de la console.

AWS CLI

Pour activer la validation de l'intégrité du fichier journal avec AWS CLI, utilisez l'`--enable-log-file-validation`option avec les commandes create-trail ou update-trail. Pour désactiver la validation de l'intégrité des fichiers journaux, utilisez l'option `--no-enable-log-file-validation`.

Example (Exemple)

La commande `update-trail` suivante active la validation des fichiers journaux et commence à livrer des fichiers de valeur de hachage dans le compartiment Amazon S3 pour le journal de suivi spécifié.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

Pour activer la validation de l'intégrité du fichier journal avec l' CloudTrail API, définissez le paramètre de `EnableLogFileValidation` demande sur `true` lors de l'appel `CreateTrail` ou`UpdateTrail`.

Pour plus d'informations, consultez CreateTrailet UpdateTraildans le Guide de référence des AWS CloudTrail API.

Validation de l'intégrité du fichier CloudTrail journal à l'aide du AWS CLI

Pour valider les journaux avec le AWS Command Line Interface, utilisez la CloudTrail `validate-logs` commande. La commande utilise les fichiers de valeur de hachage livrés dans votre compartiment Amazon S3 pour effectuer la validation. Pour plus d'informations sur les fichiers de valeur de hachage, consultez CloudTrail structure du fichier digest.

Vous AWS CLI permet de détecter les types de modifications suivants :

- Modification ou suppression de fichiers CloudTrail journaux
- Modification ou suppression de fichiers CloudTrail de synthèse
- Modification ou suppression des deux types de fichiers ci-dessus

> **Note**
>
> AWS CLI Valide uniquement les fichiers journaux référencés par des fichiers de synthèse. Pour plus d'informations, consultez Vérifier si un fichier particulier a été livré par CloudTrail.

Prérequis

Pour valider l'intégrité du fichier journal avec le AWS CLI, les conditions suivantes doivent être remplies :

- Vous devez disposer d'une connexion en ligne pour AWS.
- Vous devez disposer d'un accès en lecture au compartiment Amazon S3 qui contient les fichiers de valeur de hachage et les fichiers journaux.
- Les fichiers de synthèse et de journal ne doivent pas avoir été déplacés de l'emplacement Amazon S3 d'origine où ils ont été CloudTrail livrés.

> **Note**
>
> Les fichiers journaux qui ont été téléchargés sur le disque local ne peuvent pas être validés avec la AWS CLI. Pour des recommandations sur la création de vos propres outils pour la validation, consultez Implémentations personnalisées de validation de l'intégrité des fichiers CloudTrail journaux.

validate-logs

Syntaxe

Voici la syntaxe de `validate-logs`. Les paramètres facultatifs sont présentés entre crochets.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> La commande `validate-logs` est spécifique à la région. Vous devez spécifier l'option `--region` globale pour valider les journaux d'un utilisateur spécifique Région AWS.

Options

Voici les options de ligne de commande pour `validate-logs`. Les options `--trail-arn` et `--start-time` sont requises. L'option `--account-id` est également requise pour les journaux de suivi d'organisation.

`--start-time`

Spécifie que les fichiers journaux livrés à la valeur d'horodatage UTC spécifiée ou après seront validés. Exemple: `2015-01-08T05:21:42Z`.

`--end-time`

Spécifie en option que les fichiers journaux livrés à la valeur d'horodatage UTC spécifiée ou avant seront validés. La valeur par défaut est l'heure UTC actuelle (`Date.now()`). Exemple: `2015-01-08T12:31:41Z`.

> **Note**
>
> Pour la plage de temps spécifiée, la commande `validate-logs` vérifie uniquement les fichiers journaux qui sont référencés dans les fichiers de valeur de hachage correspondants. Aucun autre fichier journal dans le compartiment Amazon S3 n'est vérifié. Pour plus d'informations, consultez Vérifier si un fichier particulier a été livré par CloudTrail.

`--s3-bucket`

Vous pouvez également spécifier le compartiment Amazon S3 où les fichiers de valeur de hachage sont stockés. Si aucun nom de compartiment n'est spécifié, il AWS CLI sera récupéré en appelant`DescribeTrails()`.

`--s3-prefix`

Vous pouvez également spécifier le préfixe Amazon S3 où les fichiers de valeur de hachage sont stockés. S'il n'est pas spécifié, il le AWS CLI récupérera en appelant`DescribeTrails()`.

> **Note**
>
> Vous devez utiliser cette option uniquement si votre préfixe actuel est différent du préfixe utilisé au cours de la plage de temps que vous spécifiez.

`--account-id`

Spécifie éventuellement le compte pour la validation des journaux. Ce paramètre est obligatoire pour les journaux de suivi d'organisation afin de valider les journaux d'un compte spécifique au sein d'une organisation.

`--trail-arn`

Spécifie le nom Amazon Resource Name (ARN) du suivi à valider. Format de l'ARN d'un suivi.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> Pour obtenir l'ARN d'un suivi, vous pouvez utiliser la commande `describe-trails` avant d'exécuter `validate-logs`.
> Vous pouvez spécifier le nom du compartiment et le préfixe en plus de l'ARN du suivi si les fichiers journaux ont été livrés à plusieurs compartiments dans la plage de temps que vous avez spécifiée, et que vous souhaitez limiter la validation au fichiers journaux dans un seul des compartiments.

`--verbose`

Génère, en option, des informations de validation pour chaque fichier journal ou fichier de valeur de hachage dans la plage de temps spécifiée. La sortie indique si le fichier reste inchangé ou s'il a été modifié ou supprimé. En mode non détaillé (la valeur par défaut), les informations sont renvoyées uniquement en cas d'échec de validation.

Exemple

L'exemple suivant valide les fichiers journaux à partir de l'heure de début spécifiée jusqu'à l'heure actuelle, à l'aide du compartiment Amazon S3 configuré pour le journal d'activité actuel et en spécifiant une sortie détaillée.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

Fonctionnement d'**`validate-logs`**

La commande `validate-logs` commence par valider le fichier de valeur de hachage le plus récent dans la plage de temps spécifiée. Elle vérifie d'abord que le fichier de valeur de hachage a été téléchargé à partir de l'emplacement auquel il prétend appartenir. En d'autres termes, si la CLI télécharge le fichier de valeur de hachage `df1` à partir de l'emplacement S3 `p1`, validate-logs vérifie que `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`.

Si la signature du fichier de valeur de hachage est valide, elle vérifie la valeur de hachage de chacun des journaux référencés dans le fichier de valeur de hachage. La commande remonte ensuite dans le temps et valide les fichiers de valeur de hachage précédents ainsi que les fichiers journaux référencés dans l'ordre. Elle continue jusqu'à ce que la valeur spécifiée pour `start-time` soit

atteinte, ou jusqu'à la fin de chaîne de valeur de hachage prenne fin. Si un fichier de valeur de hachage est manquant ou non valide, la plage de temps ne pouvant pas être validée est indiquée dans la sortie.

Résultats de la validation

Les résultats de la validation commencent par un en-tête récapitulatif au format suivant :

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

Chaque ligne de la sortie principale contient les résultats de validation d'un fichier de valeur de hachage ou d'un fichier journal au format suivant :

```
<Digest file | Log file> <S3 path> <Validation Message>
```

Le tableau suivant décrit les messages de validation possibles pour les fichiers journaux et les fichiers de valeur de hachage.

Type de fichier	Message de validation	Description
`Digest file`	`valid`	La signature du fichier de valeur de hachage est valide. Les fichiers journaux auxquels if fait référence peuvent être vérifiés. Ce message est inclus uniquement en mode détaillé.
`Digest file`	`INVALID: has been moved from its original location`	Le compartiment S3 ou l'objet S3 à partir dont le fichier de valeur de hachage été extrait ne correspond pas aux emplaceme nts de compartiment S3 ou d'objet S3 enregistrées dans le fichier de valeur de hachage.
`Digest file`	`INVALID: invalid format`	Le format du fichier de valeur de hachage n'est pas valide. Les fichiers journaux correspondant à la plage de temps que le fichier de valeur de hachage représente ne peuvent pas être validés.

Type de fichier	Message de validation	Description
`Digest file`	`INVALID: not found`	Le fichier de valeur de hachage est introuvable. Les fichiers journaux correspondant à la plage de temps que le fichier de valeur de hachage représente ne peuvent pas être validés.
`Digest file`	`INVALID: public key not found for fingerprint` *`Empreinte digitale`*	La clé publique correspondant à l'empreinte digitale enregistrée dans le fichier de valeur de hachage est introuvable. Le fichier de valeur de hachage ne peut pas être validé.
`Digest file`	`INVALID: signature verification failed`	La signature du fichier de valeur de hachage n'est pas valide. Etant donné que le fichier de valeur de hachage n'est pas valide, les fichiers journaux auxquels il fait référence ne peuvent pas être validés et aucune affirmation ne peut être faite concernant l'activité de l'API dans ces fichiers.
`Digest file`	`INVALID: Unable to load PKCS #1 key with fingerprint` *`Empreinte digitale`*	Etant donné que la clé publique codée DER au format PKCS #1 possédant l'empreinte spécifiée n'a pas pu être chargée, le fichier de valeur de hachage ne peut pas être validé.
`Log file`	`valid`	Le fichier journal a été validé et n'a pas été modifié depuis le moment de la livraison. Ce message est inclus uniquement en mode détaillé.
`Log file`	`INVALID: hash value doesn't match`	Le hachage du fichier journal ne correspond pas. Le fichier journal a été modifié après sa livraison par CloudTrail.
`Log file`	`INVALID: invalid format`	Le format du fichier journal n'est pas valide. Le fichier journal ne peut pas être validé.

Type de fichier	Message de validation	Description
`Log file`	`INVALID: not found`	Le fichier journal est introuvable et ne peut pas être validé.

La sortie inclut des informations récapitulative sur les résultats retournés.

Exemples de sorties

Détaillée

L'exemple de commande `validate-logs` suivant utilise l'indicateur `--verbose` et produit le résultat qui suit. `[...]` indique l'exemple de sortie abrégée.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Non détaillée

L'exemple de commande `validate-logs` suivant n'utilise pas l'indicateur `--verbose`. Dans l'exemple de sortie qui suit, une erreur a été détectée. Seules les informations concernant l'en-tête, les erreurs et les informations récapitulatives sont renvoyées.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Vérifier si un fichier particulier a été livré par CloudTrail

Pour vérifier si un fichier spécifique de votre bucket a été livré par CloudTrail, exécutez-le `validate-logs` en mode détaillé pendant la période pendant laquelle le fichier est inclus. Si le fichier apparaît dans la sortie de`validate-logs`, il a été livré par CloudTrail.

CloudTrail structure du fichier digest

Chaque fichier de condensat contient les noms des fichiers journaux qui ont été livrés dans votre compartiment Amazon S3 au cours de la dernière heure, les valeurs de hachage de ces fichiers journaux, ainsi que la signature numérique du précédent fichier de condensat. La signature du fichier de condensat actuel est stocké dans les propriétés de métadonnées de l'objet fichier de condensat. Les signatures numériques et les hachages sont utilisés pour valider l'intégrité des fichiers journaux et du fichier de condensat même.

Emplacement du fichier de condensat

Les fichiers de condensat sont livrés dans un emplacement de compartiment Amazon S3 qui respecte cette syntaxe.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> Pour les journaux d'activité d'une organisation, l'emplacement du compartiment inclut également l'ID de l'unité d'organisation, comme suit :
>
> ```
> s3://s3-bucket-name/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

Exemple de contenu du fichier de condensat

L'exemple de fichier de synthèse suivant contient les informations d'un CloudTrail journal.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```


Description des champs d'un fichier de condensat

Voici la description de chacun des champs du fichier de condensat :

`awsAccountId`

L'identifiant du AWS compte pour lequel le fichier condensé a été livré.

`digestStartTime`

La plage horaire UTC de départ couverte par le fichier de synthèse, en prenant comme référence l'heure à laquelle les fichiers journaux ont été livrés CloudTrail. Cela signifie que si la plage de temps est [Ta, Tb], le condensé contiendra tous les fichiers journaux livrés au client entre Ta et Tb.

`digestEndTime`

La plage horaire UTC finale couverte par le fichier de synthèse, en prenant comme référence l'heure à laquelle les fichiers journaux ont été livrés CloudTrail. Cela signifie que si la plage de temps est [Ta, Tb], le condensé contiendra tous les fichiers journaux livrés au client entre Ta et Tb.

`digestS3Bucket`

Le nom du compartiment Amazon S3 dans lequel le fichier de condensat actuel a été livré.

`digestS3Object`

La Clé d'objet Amazon S3 (c.-à-d., emplacement du compartiment Amazon S3) du fichier de condensat actuel. Les deux premières régions dans la chaîne présentent la région à partir de laquelle le fichier de condensat a été livré. La dernière région (après `your-trail-name`) est la région d'origine du journal de suivi. La région d'origine est celle dans laquelle le journal de suivi a été créé. Dans le cas d'un journal de suivi multi-régions, elle peut être différente de la région à partir de laquelle le fichier de condensat a été livré.

`newestEventTime`

L'heure UTC de l'événement le plus récent parmi tous les événements dans les fichiers journaux dans le condensé.

`oldestEventTime`

L'heure UTC de l'événement le plus ancien parmi tous les événements dans les fichiers journaux dans le condensé.

> **Note**
>
> Si le fichier de condensat est livré en retard, la valeur de `oldestEventTime` sera antérieure à la valeur de `digestStartTime`.

`previousDigestS3Bucket`

Le Compartiment Amazon S3 dans lequel le fichier de condensat précédent a été livré.

`previousDigestS3Object`

La Clé d'objet Amazon S3 (c.-à-d., emplacement du compartiment Amazon S3) du fichier de condensat précédent.

`previousDigestHashValue`

La valeur de hachage codée hexadécimale du contenu non compressé du fichier de condensat précédent.

`previousDigestHashAlgorithm`

Le nom de l'algorithme de hachage utilisé pour hacher le fichier de condensat précédent.

`publicKeyFingerprint`

L'empreinte codée au format hexadécimal de la clé publique qui correspond à la clé privée utilisée pour signer ce fichier de condensat. Vous pouvez récupérer les clés publiques pour la plage de temps correspondant au fichier condensé à l'aide de l'API AWS CLI ou de l' CloudTrail API. Parmi les clés publiques renvoyées, celle dont l'empreinte correspond à cette valeur peut être utilisée pour valider le fichier de condensat. Pour plus d'informations sur la récupération des clés publiques pour les fichiers de synthèse, consultez la AWS CLI `list-public-keys`commande ou l' CloudTrail `ListPublicKeys`API.

> **Note**
>
> CloudTrail utilise différentes paires de clés privées/publiques par région. Chaque fichier de condensat est signé avec une clé privée unique à sa région. Par conséquent, lorsque

vous validez un fichier de condensat provenant d'une région donnée, vous devez rechercher dans la même région la clé publique correspondante.

`digestSignatureAlgorithm`

L'algorithme utilisé pour signer le fichier de condensat.

`logFiles.s3Bucket`

Le nom du compartiment Amazon S3 contenant le fichier journal.

`logFiles.s3Object`

La clé d'objet Amazon S3 du fichier journal actuel.

`logFiles.newestEventTime`

L'heure UTC de l'événement le plus récent dans le fichier journal. Cette heure correspond aussi à l'horodatage du fichier journal même.

`logFiles.oldestEventTime`

L'heure UTC de l'événement le plus ancien dans le fichier journal.

`logFiles.hashValue`

La valeur de hachage codée au format hexadécimal du contenu du fichier journal décompressé.

`logFiles.hashAlgorithm`

L'algorithme de hachage utilisé pour hacher le fichier journal.

Fichier de condensat de départ

Au démarrage de la validation de l'intégrité des fichiers journaux, un fichier de condensat de départ sera généré. Un fichier de condensat de départ sera également généré au redémarrage de la validation de l'intégrité des fichiers journaux (soit en désactivant puis en réactivant la validation de

l'intégrité des fichiers journaux ou en arrêtant puis en redémarrant la journalisation avec la validation activée). Dans un fichier de condensat de départ, les champs suivants concernant le fichier de condensat précédent auront la valeur nulle :

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

Fichiers de condensat « vides »

CloudTrail fournira un fichier de résumé même s'il n'y a eu aucune activité d'API sur votre compte pendant la période d'une heure représentée par le fichier de résumé. Cela peut être utile lorsque vous avez besoin d'affirmer qu'aucun fichier journal n'a été livré au cours de l'heure signalé par le fichier de condensat.

L'exemple suivant présente le contenu d'un fichier de condensat qui a enregistré une heure alors qu'aucune activité d'API ne s'est produite. Notez que le champ `logFiles:[ ]` à la fin du contenu du fichier de condensat est vide.


```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
```

```
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```

Signature du fichier de condensat

Les informations de signature d'un fichier de condensat sont contenues dans deux propriétés de métadonnées de l'objet du fichier de condensat Amazon S3. Chaque fichier de condensat contient les entrées de métadonnées suivantes :

- `x-amz-meta-signature`

  La valeur codée au format hexadécimal de la signature du fichier de condensat. Voici un exemple de signature :

  ```
  3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
  28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
  05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
  ```

- `x-amz-meta-signature-algorithm`

  Ci-après, un exemple de valeur de l'algorithme utilisé pour générer la signature du condensé :

  `SHA256withRSA`

Chaînage du fichier de condensat

Le fait que chaque fichier de résumé contienne une référence à son précédent fichier de résumé permet un « chaînage » qui permet à des outils de validation tels que le de AWS CLI détecter si un fichier de résumé a été supprimé. Il autorise également l'inspection des fichiers de condensat contenus dans une plage de temps donnée successivement, en commençant par le plus récent.

> **Note**
>
> Lorsque vous désactivez la validation de l'intégrité des fichiers journaux, la chaîne des fichiers de synthèse est interrompue au bout d'une heure. CloudTrail ne créera pas de fichiers de synthèse pour les fichiers journaux fournis pendant une période pendant laquelle

la validation de l'intégrité des fichiers journaux était désactivée. Par exemple, si vous activez la validation de l'intégrité de fichiers journaux à midi le 1er janvier, que vous la désactiviez le 2 janvier à midi et la réactiviez le 10 janvier à midi, les fichiers de condensat ne seront pas créés pour les fichiers journaux livrés du 2 janvier à midi au 10 janvier à midi. Il en va de même chaque fois que vous CloudTrail arrêtez de consigner ou supprimez un parcours.

Si la politique de compartiment S3 de votre sentier est mal configurée ou si elle CloudTrail subit une interruption de service inattendue, il est possible que vous ne receviez pas tous les fichiers de résumé ou certains d'entre eux. Pour vérifier si votre journal contient des erreurs de livraison du résumé, exécutez la `get-trail-status`commande et vérifiez l'absence d'erreurs dans le `LatestDigestDeliveryError` paramètre. Une fois le problème de livraison résolu (par exemple, en corrigeant la politique relative aux compartiments), CloudTrail tentera de renvoyer les fichiers de résumé manquants. Au cours de la période de relivraison, les fichiers du résumé peuvent être livrés en rupture de commande, de sorte que la chaîne peut sembler temporairement interrompue.

Si la journalisation est arrêtée ou si le journal est supprimé, un fichier de résumé final CloudTrail sera fourni. Ce fichier de condensat peut contenir des informations concernant tout fichier journal restant qui couvre des événements jusqu'à et y compris l'événement `StopLogging`.

Implémentations personnalisées de validation de l'intégrité des fichiers CloudTrail journaux

Grâce à l' CloudTrail utilisation d'algorithmes cryptographiques et de fonctions de hachage conformes aux normes du secteur et librement disponibles, vous pouvez créer vos propres outils pour valider l'intégrité des fichiers CloudTrail journaux. Lorsque la validation de l'intégrité des fichiers journaux est activée, CloudTrail les fichiers de synthèse sont envoyés à votre compartiment Amazon S3. Vous pouvez utiliser ces fichiers pour implémenter votre propre solution de validation. Pour plus d'informations sur les fichiers de valeur de hachage, consultez la page CloudTrail structure du fichier digest.

Cette rubrique explique comment les fichiers de valeur de hachage sont signées, puis détaille les étapes nécessaires pour implémenter une solution qui valide les fichiers de valeur de hachage et les fichiers journaux auxquels ils font référence.

Comprendre comment les CloudTrail fichiers de synthèse sont signés

CloudTrail les fichiers de synthèse sont signés avec des signatures numériques RSA. Pour chaque fichier de résumé, CloudTrail effectue les opérations suivantes :

1. Crée une chaîne pour la signature des données basée sur les champs de fichier de valeur de hachage désignés (décrits dans la section suivante).
2. Obtient une clé privée unique pour la région.
3. Transmet le hachage SHA-256 de la chaîne et la clé privée de l'algorithme de signature RSA, qui génèrent une signature numérique.
4. Code le code d'octet de la signature dans un format hexadécimal.
5. Place la signature numérique dans la propriété de métadonnées `x-amz-meta-signature` de l'objet de fichier de valeur de hachage Amazon S3.

Contenu de la chaîne de signature des données

Les CloudTrail objets suivants sont inclus dans la chaîne pour la signature des données :

- L'horodatage de fin du fichier de valeur de hachage au format UTC étendu (par exemple, `2015-05-08T07:19:37Z`)
- Chemin d'accès du fichier de valeur de hachage S3 actuel
- Hachage SHA-256 codé au format hexadécimal du fichier de valeur de hachage actuel
- Signature codée au format hexadécimal du fichier de valeur de hachage précédent

Le format pour le calcul de cette chaîne et un exemple de chaîne sont fournis ultérieurement dans ce document.

Étapes d'implémentation de la validation personnalisée

Lors de l'implémentation d'une solution de validation personnalisée, vous devez d'abord valider le fichier de valeur de hachage, puis les fichiers journaux auxquels il fait référence.

Valider le fichier de valeur de hachage

Afin de valider un fichier de valeur de hachage, vous avez besoin de sa signature, de la clé publique dont la clé privée a été utilisée pour le signer et d'une chaîne de signature des données que vous calculez.

1. Obtenir le fichier de valeur de hachage.
2. Vérifier que le fichier de valeur de hachage a été récupéré à partir de son emplacement d'origine.
3. Obtenir la signature codée au format hexadécimal du fichier de valeur de hachage.
4. Obtenir l'empreinte codée au format hexadécimal de la clé publique dont la clé privée a été utilisée pour signer le fichier de valeur de hachage.
5. Récupérer les clés publiques pour la plage de temps correspondant au fichier de valeur de hachage.
6. Parmi les clés publiques récupérées, sélectionnez la clé publique dont l'empreinte correspond à l'empreinte dans le fichier de valeur de hachage.
7. Grâce au hachage du fichier de valeur de hachage et aux autres champs du fichier de valeur de hachage, recréer la chaîne de signature utilisée pour vérifier la signature de fichier de valeur de hachage.
8. Valider la signature en transmettant le hachage SHA-256 de la chaîne, la clé publique et la signature comme paramètres de l'algorithme de vérification de signature RSA. Si le résultat est true, le fichier de valeur de hachage est valide.

Valider les fichiers-journaux

Si le fichier de valeur de hachage est valide, valider chacun des fichiers journaux auquel le fichier de valeur de hachage fait référence.

1. Afin de valider l'intégrité d'un fichier journal, calculer sa valeur de hachage SHA-256 sur son contenu décompressé et comparer les résultats avec le hachage du fichier journal enregistré au format hexadécimal dans la valeur de hachage. Si les hachages correspondent, le fichier journal est valide.
2. En utilisant les informations concernant le fichier de valeur de hachage précédent qui est inclus dans le fichier de valeur de hachage actuel, valider les fichiers de valeur de hachage précédents et leurs journaux correspondants dans l'ordre.

Les sections suivantes décrivent ces étapes en détail.

Obtenir le fichier de valeur de hachage.

Les premières étapes consistent à obtenir le fichier de valeur de hachage le plus récent, vérifier que vous l'avez récupéré de son emplacement d'origine, vérifier sa signature numérique et obtenir l'empreinte de la clé publique.

1. À l'aide de S3 `GetObject`ou de la classe AmazonS3Client (par exemple), récupérez le fichier condensé le plus récent de votre compartiment Amazon S3 pour la période que vous souhaitez valider.
2. Vérifiez que le compartiment S3 et l'objet S3 utilisés pour récupérer le fichier correspondent aux emplacements du compartiment S3 et de l'objet S3 qui sont enregistrés dans le fichier de valeur de hachage même.
3. Obtenez ensuite la signature numérique du fichier de valeur de hachage à partir de la propriété de métadonnées `x-amz-meta-signature` de l'objet du fichier de valeur de hachage dans Amazon S3.
4. Dans le fichier de valeur de hachage, obtenez l'empreinte de la clé publique dont la clé privée a été utilisée pour signer le fichier de valeur de hachage à partir du champ `digestPublicKeyFingerprint`.

B. Récupérer la clé publique pour valider le fichier de valeur de hachage

Pour obtenir la clé publique permettant de valider le fichier condensé, vous pouvez utiliser l'API AWS CLI ou l' CloudTrail API. Dans les deux cas, vous spécifiez une plage de temps (c'est-à-dire, une heure de début et une heure de fin) pour les fichiers de valeur de hachage que vous voulez valider. Une ou plusieurs clés publiques peuvent être retournées pour l'intervalle de temps que vous spécifiez. Les clés renvoyées peuvent avoir des plages de temps de validité qui se chevauchent.

> **Note**
>
> Comme il CloudTrail utilise différentes paires de clés privées/publiques par région, chaque fichier condensé est signé avec une clé privée propre à sa région. Par conséquent, lorsque vous validez un fichier de valeur de hachage à partir d'une région donnée, vous devez récupérer sa clé publique à partir de la même région.

Utilisez le AWS CLI pour récupérer les clés publiques

Pour récupérer les clés publiques des fichiers de synthèse à l'aide de AWS CLI, utilisez la `cloudtrail list-public-keys` commande. La commande a le format suivant :

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Les paramètres d'heure de début et d'heure de fin sont des horodatages UTC facultatifs. S'ils ne sont pas spécifiés, l'heure actuelle est utilisée et la ou les clés publiques actives sont renvoyées.

Exemple de réponse

La réponse est une liste d'objets JSON représentant la (ou les) clé(s) renvoyées :


```
{
    "publicKeyList": [
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

Utiliser l' CloudTrail API pour récupérer les clés publiques

Pour récupérer les clés publiques des fichiers de synthèse à l'aide de l' CloudTrail API, transmettez les valeurs d'heure de début et de fin à l'`ListPublicKeys`API. L'API `ListPublicKeys` retourne les clés publiques dont les clés privées ont été utilisés pour signer les fichiers de valeur de hachage dans la plage de temps spécifiée. Pour chaque clé publique, l'API renvoie également l'empreinte correspondante.

`ListPublicKeys`

Cette section décrit les paramètres de demande et les éléments de réponse pour l'API `ListPublicKeys`.

> **Note**
>
> L'encodage pour les champs binaires pour `ListPublicKeys` est susceptible d'être modifié.

Paramètres de requête

Name (Nom)	Description
`StartTime`	Spécifie éventuellement, en UTC, le début de la plage de temps pour rechercher les clés publiques des fichiers de CloudTrail résumé. Si StartTime ce n'est pas spécifié, l'heure actuelle est utilisée et la clé publique actuelle est renvoyée. Type : DateTime
`EndTime`	Spécifie éventuellement, en UTC, la fin de la plage de temps pour rechercher les clés publiques pour les fichiers de CloudTrail résumé. Si EndTime ce n'est pas spécifié, l'heure actuelle est utilisée. Type : DateTime

Éléments de réponse

`PublicKeyList`, un tableau des objets `PublicKey` qui contient les éléments suivants :

Name (Nom)	Description
`Value`	La valeur de clé publique codée DER au format PKCS #1. Type : Blob
`ValidityStartTime`	Heure de début de validité de la clé publique. Type : DateTime
`ValidityEndTime`	Heure de fin de validité de la clé publique. Type : DateTime
`Fingerprint`	Empreinte de la clé publique. L'empreinte peut servir à identifier la clé publique que vous devez utiliser pour valider le fichier de valeur de hachage. Type : chaîne

C. Sélectionner la clé publique à utiliser pour la validation

Parmi les clés publiques récupérées par `list-public-keys` ou `ListPublicKeys`, sélectionnez la clé publique renvoyée dont l'empreinte correspond à l'empreinte enregistrée dans le champ du fichier de valeur de hachage `digestPublicKeyFingerprint`. C'est la clé publique que vous utiliserez pour valider le fichier de valeur de hachage.

D. Recréer la chaîne de signature des données

Maintenant que vous avez la signature du fichier de valeur de hachage et la clé publique associée, vous devez calculer la chaîne de signature des données. Une fois que vous aurez calculé les chaîne de signature des données, vous aurez les entrées nécessaires pour vérifier la signature.

La chaîne de signature des données possède le format suivant :

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

Un exemple de `Data_To_Sign_String` suit.

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

Une fois que vous avez recréé cette chaîne, vous pouvez valider le fichier de valeur de hachage.

E. Valider le fichier de valeur de hachage

Transmettez le hachage SHA-256 de la chaîne de signature de données recréée, la signature numérique et la clé publique de l'algorithme de vérification de la signature RSA. Si le résultat est true, la signature du fichier de valeur de hachage est vérifiée et le fichier de valeur de hachage est valide.

F. Valider les fichiers-journaux

Une fois que vous avez validé le fichier de valeur de hachage, vous pouvez valider les fichiers-journaux auquel il fait référence. Le fichier de valeur de hachage contient les hachages SHA-256 des fichiers journaux. Si l'un des fichiers journaux a été modifié après l'avoir CloudTrail livré, les hachages SHA-256 seront modifiés et la signature du fichier condensé ne correspondra pas.

La section suivante montre comment valider les fichiers journaux :

1. Exécutez la commande `S3 Get` sur le fichier journal en utilisant les informations d'emplacement S3 contenues dans les champs `logFiles.s3Bucket` et `logFiles.s3Object` du fichier valeur de hachage.
2. Si l'opération `S3 Get` est réussie, parcourez les fichiers journaux répertoriés dans le tableau de fichiers journaux du fichier de valeur de hachage en appliquant la procédure suivante :
   a. Récupérez le hachage d'origine du fichier à partir du champ `logFiles.hashValue` du journal correspondant dans le fichier de valeur de hachage.
   b. Hachez le contenu non compressé du fichier journal avec l'algorithme de hachage spécifié dans `logFiles.hashAlgorithm`.

c. Comparez la valeur de hachage que vous avez générée avec celle du fichier journal dans le fichier de valeur de hachage. Si les hachages correspondent, le fichier journal est valide.

G. Valider des fichiers de valeur de hachage et des fichiers journaux supplémentaires

Dans chaque fichier de valeur de hachage, les champs suivants fournissent l'emplacement et la signature du fichier de valeur de hachage précédent :

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

Utilisez ces informations pour consulter les fichiers de valeur de hachage précédents dans l'ordre, en validant la signature de chacun et les fichiers journaux auxquels ils font référence en appliquant la procédure présentée dans les sections précédentes. La seule différence est que pour les fichiers de valeur de hachage précédents, vous n'aviez pas besoin de récupérer la signature numérique depuis les propriétés de métadonnées Amazon S3 de l'objet du fichier de valeur de hachage. La signature du fichier de valeur de hachage précédent est fournie dans le champ `previousDigestSignature`.

Vous pouvez retourner en arrière jusqu'au fichier de valeur de hachage de départ ou jusqu'à ce que la chaîne de fichiers de valeur de hachage soit rompue, selon la première de ces deux éventualités.

Validation des fichiers de valeur de hachage et des fichiers journaux hors connexion

Lors de la validation des fichiers de valeur de hachage et des fichiers journaux hors connexion, vous pouvez généralement suivre les procédures décrites dans les sections précédentes. Cependant, vous devez prendre en compte les points suivants :

Gestion du fichier de valeur de hachage le plus récent

La signature numérique du fichier de valeur de hachage le plus récent (c'est-à-dire, « actuel ») est contenue dans les propriétés de métadonnées Amazon S3 de l'objet du fichier de valeur de hachage. Dans un scénario hors connexion, la signature numérique du fichier de valeur de hachage actuel n'est pas disponible.

Il existe deux façons de gérer cette situation :

- La signature numérique du précédent fichier condensé se trouvant dans le fichier condensé actuel, commencez à valider à partir du fichier next-to-last condensé. Avec cette méthode, le fichier de valeur de hachage le plus récent ne peut pas être validé.
- Comme étape préliminaire, obtenez la signature du fichier de valeur de hachage actuel à partir des propriétés de métadonnées de l'objet du fichier de valeur de hachage, puis stockez-la en toute sécurité hors connexion. Cela permettrait la validation du fichier actuel de valeur de hachage en plus des fichiers précédents de la chaîne.

Résolution du chemin

Les champs des fichiers de valeur de hachage téléchargés tels que `s3object` et `previousDigestS3object` continuent de pointer vers les emplacements en ligne Amazon S3 des fichiers journaux et des fichiers de valeur de hachage. Une solution hors connexion doit trouver un moyen de les réacheminer vers le chemin actuel du journal et des fichiers de valeur de hachage téléchargés.

Clés publiques

Pour effectuer une validation hors connexion, vous devez dans un premier temps obtenir toutes les clés publiques dont vous avez besoin pour valider les fichiers journaux dans une plage de temps donnée (en appelant `ListPublicKeys`, par exemple), puis les stocker en toute sécurité hors connexion. Cette étape doit être répétée chaque fois que vous souhaitez valider des fichiers supplémentaires en dehors de la plage de temps que vous avez spécifiée au départ.

Extrait de code de validation

L'exemple d'extrait suivant fournit un code squelette pour valider les fichiers de CloudTrail résumé et de journal. Ce squelette de code peut aussi bien être implémenter avec ou sans connexion à AWS ; c'est à vous de décider. L'implémentation suggéré utilise le Java Cryptography Extension (JCE) et Bouncy Castle comme fournisseur de sécurité.

L'exemple d'extrait de code montre :

- Procédure de création de la chaine de signature de données utilisée pour valider la signature du fichier de valeur de hachage des données.
- Procédure de vérification de la signature du fichier de valeur de hachage.
- Procédure de vérification des hachages de fichier journal.
- Structure de code pour la validation d'une chaîne de fichiers de valeur de hachage.

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
 digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
 as part of the data to sign
```

```
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:

                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
```

```
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
                    messageDigest.update(logFileContent);
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
```

```
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail exemples de fichiers journaux

CloudTrail surveille les événements liés à votre compte. Si vous créez un journal d'activité, celui-ci fournit ces événements sous forme de fichiers journaux dans votre compartiment Amazon S3. Si vous créez un magasin de données d'événements dans CloudTrail Lake, les événements sont enregistrés dans votre magasin de données d'événements. Les stockages de données d'événement n'utilisent pas de compartiments S3.

Rubriques

- CloudTrail format du nom du fichier journal
- Exemples de fichier journal

CloudTrail format du nom du fichier journal

CloudTrail utilise le format de nom de fichier suivant pour les objets du fichier journal qu'il fournit à votre compartiment Amazon S3 :

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYY, MM, DD, HH et mm correspondent aux chiffres de l'année, du mois, du jour, de l'heure et de la minute où le fichier journal a été remis. Les heures sont au format 24 heures. Z indique que l'heure est au format UTC.

> **Note**
>
> Un fichier journal fourni à un moment spécifique peut contenir des registres écrits n'importe quand avant ce moment.

- Le composant `UniqueString` à 16 caractères du nom du fichier journal est destiné à empêcher l'écrasement des fichiers. Il n'a aucune signification, et doit être ignoré par les logiciels de traitement des journaux.
- `FileNameFormat` correspond à l'encodage du fichier. Actuellement, c'est `json.gz`, qui est un fichier de texte JSON au format compressé gzip.

Exemple de nom de fichier CloudTrail journal

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

Exemples de fichier journal

Un fichier journal contient un ou plusieurs registres. Les exemples suivants sont des extraits de journaux qui présentent les registres correspondant à une action qui a démarré la création d'un fichier journal.

Pour plus d'informations sur les champs d'enregistrement d' CloudTrail événements, consultezCloudTrail enregistrer le contenu.

Table des matières

Exemples de journaux Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) offre une capacité de calcul redimensionnable dans l' AWS Cloud. Vous pouvez lancer autant de serveurs virtuels, configurer la sécurité et la mise en réseau, et gérer le stockage. Amazon EC2 vous permet d'augmenter ou de diminuer rapidement

l'échelle afin de gérer les modifications en termes d'exigences ou de pics de popularité, et réduire ainsi le besoin de prédire le trafic sur le serveur. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

L'exemple suivant montre qu'un utilisateur IAM nommé `Mateo` a exécuté la commande aws ec2 start-instances pour appeler l'action Amazon EC2 `StartInstances` pour les instances `i-EXAMPLE56126103cb` et `i-EXAMPLEaff4840c22`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
```

```
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
```

```
}]}
```

L'exemple suivant montre qu'un utilisateur IAM nommé `Nikki` a exécuté la commande aws ec2 stop-instances pour appeler l'action Amazon EC2 `StopInstances` pour arrêter deux instances.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
```

```
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

L'exemple suivant montre qu'un utilisateur IAM nommé `Arnav` a exécuté la commande aws ec2 create-key-pair pour appeler l'action `CreateKeyPair`. Notez qu'ils `responseElements` contiennent un hachage de la paire de clés et que cela a AWS supprimé le matériau clé.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
```

```
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


Exemples de journal IAM

AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources. Avec IAM, vous pouvez gérer de manière centralisée les autorisations qui contrôlent les ressources AWS auxquelles les utilisateurs peuvent accéder. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources. Pour plus d'informations, consultez le Guide de l'utilisateur IAM.

L'exemple suivant montre qu'un utilisateur IAM nommé `Mary` a exécuté la commande aws iam create-user pour appeler l'action `CreateUser` pour créer un utilisateur nommé `Richard`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


L'exemple suivant montre qu'un utilisateur IAM nommé `Paulo` a exécuté la commande aws iam add-user-to-group pour appeler l'action [AddUserToGroup](#) pour ajouter un utilisateur nommé `Jane` au groupe `Admin`.


```
{"Records": [{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

L'exemple suivant montre qu'un utilisateur IAM nommé `Saanvi` a exécuté la commande aws iam create-role pour appeler l'action `CreateRole` pour créer un rôle.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
```

```
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Exemple de code d'erreur et de journal de messages

L'exemple suivant montre qu'un utilisateur IAM nommé `Terry` a exécuté la commande aws cloudtrail update-trail pour appeler l'action `UpdateTrail` pour mettre à jour un journal de suivi nommé `myTrail2`, mais le nom du journal de suivi était introuvable. Le journal affiche cette erreur dans les éléments `errorCode` et `errorMessage`.

```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail Exemple de journal d'événements Insights

L'exemple suivant montre un journal CloudTrail des événements Insights. Un événement Insights est en fait une paire d'événements qui marquent le début et la fin d'une période d'activité inhabituelle de l'API de gestion d'écriture ou de réponse aux erreurs. Le champ `state` indique si l'événement a été journalisé au début ou à la fin de la période d'activité inhabituelle. Le nom de l'événement est le même que celui de l' AWS Systems Manager API pour laquelle les événements de gestion CloudTrail ont été analysés afin de déterminer si une activité inhabituelle s'est produite. `UpdateInstanceInformation` Bien que les événements de début et de fin aient des valeurs `eventID` uniques, ils ont également une valeur `sharedEventID` qui est utilisée par la paire. L'événement Insights affiche la valeur `baseline`, soit le schéma normal d'activité, la valeur `insight`, soit l'activité moyenne inhabituelle qui a déclenché l'événement Insights de début

et, dans l'événement de fin, la valeur `insight` correspondant à l'activité moyenne inhabituelle pendant toute la durée de l'événement Insights. Pour plus d'informations sur CloudTrail Insights, consultezJournalisation des événements Insights.


```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
```

```
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

Utilisation de la bibliothèque CloudTrail de traitement

La bibliothèque de CloudTrail traitement est une bibliothèque Java qui permet de traiter facilement AWS CloudTrail les journaux. Vous fournissez les détails de configuration de votre file d'attente CloudTrail SQS et vous écrivez du code pour traiter les événements. La bibliothèque CloudTrail de traitement s'occupe du reste. Il interroge votre file d'attente Amazon SQS, lit et analyse les messages de file d'attente, télécharge les fichiers CloudTrail journaux, analyse les événements contenus dans les fichiers journaux et transmet les événements à votre code sous forme d'objets Java.

La bibliothèque CloudTrail de traitement est hautement évolutive et tolérante aux pannes. Elle gère le traitement parallèle des fichiers journaux de telle sorte que vous puissiez traiter autant de journaux que nécessaire. Elle gère les défaillances du réseau liées aux délais de réseau et aux ressources inaccessibles.

La rubrique suivante explique comment utiliser la bibliothèque de CloudTrail traitement pour traiter CloudTrail les journaux dans vos projets Java.

La bibliothèque est fournie sous forme de projet open source sous licence Apache, disponible sur :. GitHub https://github.com/aws/aws-cloudtrail-processing-library La source de la bibliothèque contient des exemples de code que vous pouvez utiliser comme base pour vos propres projets.

Rubriques

- Configuration requise

Configuration requise

Pour utiliser la bibliothèque CloudTrail de traitement, vous devez disposer des éléments suivants :

- AWS SDK for Java 1,1830
- Java 1.8 (Java SE 8)

CloudTrail Journaux de traitement

Pour traiter CloudTrail les journaux dans votre application Java :

1. Ajouter la bibliothèque CloudTrail de traitement à votre projet
2. Configuration de la bibliothèque CloudTrail de traitement
3. Implémentation du processeur des événements
4. Instanciation et traitement de l'exécution de traitement

Ajouter la bibliothèque CloudTrail de traitement à votre projet

Pour utiliser la bibliothèque CloudTrail de traitement, ajoutez-la au chemin de classe de votre projet Java.

Table des matières

Ajout de la bibliothèque à un projet Apache Ant

Pour ajouter la bibliothèque CloudTrail de traitement à un projet Apache Ant

1. Téléchargez ou clonez le code source de la bibliothèque de CloudTrail traitement depuis GitHub :

   - https://github.com/aws/ aws-cloudtrail-processing-library

2. Créez le fichier .jar à partir de la source comme décrit dans la section README (LISEZ-MOI) :

```
mvn clean install -Dgpg.skip=true
```

3. Copiez le fichier .jar résultant dans votre projet et ajoutez-le au fichier `build.xml` de votre projet. Par exemple :

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

Ajout de la bibliothèque à un projet Apache Maven

La bibliothèque CloudTrail de traitement est disponible pour Apache Maven. L'ajouter à votre projet est aussi simple que d'écrire une seule dépendance dans le fichier `pom.xml` de votre projet.

Pour ajouter la bibliothèque CloudTrail de traitement à un projet Maven

- Ouvrez le fichier `pom.xml` du projet Maven et ajoutez les dépendances suivantes :

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

Ajout de la bibliothèque à un projet Eclipse

Pour ajouter la bibliothèque CloudTrail de traitement à un projet Eclipse

1. Téléchargez ou clonez le code source de la bibliothèque de CloudTrail traitement depuis GitHub :
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. Créez le fichier .jar à partir de la source comme décrit dans la section README (LISEZ-MOI) :

```
mvn clean install -Dgpg.skip=true
```

3. Copiez le fichier aws-cloudtrail-processing-library -1.6.1.jar intégré dans un répertoire de votre projet (généralement). `lib`
4. Cliquez avec le bouton droit sur le nom de votre projet dans l'Explorateur de projets Eclipse, choisissez Build Path, puis Configure
5. Dans la fenêtre Java Build Path, cliquez sur l'onglet Libraries.
6. Choisissez Ajouter des fichiers JAR... et naviguez jusqu'au chemin où vous avez copié aws-cloudtrail-processing-library -1.6.1.jar.
7. Cliquez sur OK pour terminer l'ajout du fichier `.jar` à votre projet.

Ajout de la bibliothèque à un projet IntelliJ

Pour ajouter la bibliothèque CloudTrail de traitement à un projet IntelliJ

1. Téléchargez ou clonez le code source de la bibliothèque de CloudTrail traitement depuis GitHub :
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. Créez le fichier .jar à partir de la source comme décrit dans la section README (LISEZ-MOI) :

```
mvn clean install -Dgpg.skip=true
```

3. Dans File, choisissez Projet Structure.
4. Choisissez Modules, puis Dependencies.
5. Choisissez + JARS ou Répertoires, puis accédez au chemin où vous avez créé le fichier `aws-cloudtrail-processing-library-1.6.1.jar`.

6. Choisissez Apply (Appliquer), puis cliquez sur OK pour terminer l'ajout du `.jar` à votre projet.

Configuration de la bibliothèque CloudTrail de traitement

Vous pouvez configurer la bibliothèque de CloudTrail traitement en créant un fichier de propriétés de chemin de classe chargé lors de l'exécution, ou en créant un `ClientConfiguration` objet et en définissant les options manuellement.

Fourniture d'un fichier de propriétés

Vous pouvez écrire un fichier de propriétés de chemin de classe qui fournit des options de configuration à votre application. L'exemple suivant montre les options que vous pouvez définir :

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
```

```
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

Les paramètres suivants sont obligatoires :

- `sqsUrl`— Fournit l'URL à partir de laquelle vous pouvez extraire vos CloudTrail notifications. Si vous ne spécifiez pas cette valeur, `AWSCloudTrailProcessingExecutor` lève une `IllegalStateException`.
- `accessKey` : Identifiant unique pour votre compte, comme .AKIAIOSFODNN7EXAMPLE.
- `secretKey`— Un identifiant unique pour votre compte, tel que bPxRfi WJALRxUTNFEMI/ K7MDENG/CYEXAMPLEKEY.

Les `secretKey` paramètres `accessKey` et fournissent vos AWS informations d'identification à la bibliothèque afin que celle-ci puisse y accéder AWS en votre nom.

Les paramètres par défaut pour les autres paramètres sont définis par la bibliothèque. Pour plus d'informations, consultez la Référence de bibliothèque de traitement AWS CloudTrail.

Création d'un ClientConfiguration

Au lieu de définir les options dans les propriétés de chemin de classe, vous pouvez fournir des options à la classe `AWSCloudTrailProcessingExecutor` en initialisant et en définissant des options dans un objet `ClientConfiguration`, comme indiqué dans l'exemple suivant :

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

Implémentation du processeur des événements

Pour traiter CloudTrail les journaux, vous devez implémenter un `EventsProcessor` système qui reçoit les données des CloudTrail journaux. Voici un exemple d'implémentation :

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

Lorsque vous implémentez un`EventsProcessor`, vous implémentez le `process()` rappel qu'il `AWSCloudTrailProcessingExecutor` utilise pour vous envoyer CloudTrail des événements. Les événements sont fournis dans une liste d'objets `CloudTrailClientEvent`.

L'`CloudTrailClientEvent`objet fournit un `CloudTrailEvent` et `CloudTrailEventMetadata` que vous pouvez utiliser pour lire les informations relatives à l' CloudTrail événement et à la livraison.

Cet exemple simple imprime les informations d'événement pour chaque événement transmis à `SampleEventsProcessor`. Dans votre propre implémentation, vous pouvez traiter les journaux selon vos besoins. L'objet `AWSCloudTrailProcessingExecutor` continue à envoyer des événements à votre `EventsProcessor` tant que celui-ci contient des événements d'envoi et qu'il est en cours d'exécution.

Instanciation et traitement de l'exécution de traitement

Après avoir écrit `EventsProcessor` et défini les valeurs de configuration de la bibliothèque de CloudTrail traitement (soit dans un fichier de propriétés, soit à l'aide de la `ClientConfiguration` classe), vous pouvez utiliser ces éléments pour initialiser et utiliser un`AWSCloudTrailProcessingExecutor`.

À utiliser **`AWSCloudTrailProcessingExecutor`** pour traiter CloudTrail des événements

1. Instanciez un objet `AWSCloudTrailProcessingExecutor.Builder`. Le constructeur du `Builder` prend un objet `EventsProcessor` et un nom de fichier de propriétés de chemin de classe.

2. Appelez la méthode factory `Builder` de l'objet `build()` pour configurer et obtenir un objet `AWSCloudTrailProcessingExecutor`.
3. Utilisez les `AWSCloudTrailProcessingExecutor` `stop()` méthodes `start()` et les méthodes pour démarrer et terminer le traitement des CloudTrail événements.

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

Rubriques avancées

Rubriques

- Filtration des événements à traiter
- Traitement des événements de données
- Rapports d'avancement
- Gestion des erreurs

Filtration des événements à traiter

Par défaut, tous les journaux contenus dans le compartiment S3 de la file d'attente Amazon SQS et tous les événements qu'ils contiennent sont envoyés à l'objet `EventsProcessor`. La bibliothèque de CloudTrail traitement fournit des interfaces facultatives que vous pouvez implémenter pour filtrer les sources utilisées pour obtenir les CloudTrail journaux et pour filtrer les événements que vous souhaitez traiter.

`SourceFilter`

Vous pouvez implémenter l'interface `SourceFilter` pour choisir si vous souhaitez traiter les journaux provenant d'une source fournie. `SourceFilter` déclare une méthode de rappel unique,

`filterSource()`, qui reçoit un objet `CloudTrailSource`. Pour conserver des événements provenant d'une source en cours de traitement, renvoyez la valeur `false` de `filterSource()`.

La bibliothèque CloudTrail de traitement appelle la `filterSource()` méthode une fois qu'elle a demandé des journaux dans la file d'attente Amazon SQS. Cet événement se produit avant que la bibliothèque commence le filtrage ou le traitement des journaux.

Voici un exemple d'implémentation :

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

Si vous ne fournissez pas votre propre `SourceFilter`, `DefaultSourceFilter` est alors utilisé, ce qui permet de traiter toutes les sources (renvoie toujours la valeur `true`).

`EventFilter`

Vous pouvez implémenter l'`EventFilter`interface pour choisir si un CloudTrail événement est envoyé à votre`EventsProcessor`. `EventFilter`déclare une méthode de rappel unique`filterEvent()`, qui reçoit un `CloudTrailEvent` objet. Pour empêcher le traitement de l'événement, renvoyez la valeur `false` à partir de la méthode `filterEvent()`.

La bibliothèque CloudTrail de traitement appelle la `filterEvent()` méthode après avoir demandé des journaux dans la file d'attente Amazon SQS et après le filtrage des sources. Cet événement se produit avant que la bibliothèque commence le traitement des journaux.

Voir l'exemple d'implémentation suivant :

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

Si vous ne fournissez pas votre propre `EventFilter`, `DefaultEventFilter` est alors utilisé, ce qui permet de traiter tous les événements (renvoie toujours la valeur `true`).

Traitement des événements de données

Lors du CloudTrail traitement des événements de données, il conserve les nombres dans leur format d'origine, qu'il s'agisse d'un entier (`int`) ou d'un `float` (un nombre contenant une décimale). Dans les événements contenant des nombres entiers dans les champs d'un événement de données, ces nombres CloudTrail étaient traditionnellement traités comme des nombres flottants. Actuellement, CloudTrail traite les numéros dans ces champs en conservant leur format d'origine.

Pour éviter de perturber vos automatisations, faites preuve de flexibilité dans le code ou l'automatisation que vous utilisez pour traiter ou filtrer les événements liés aux CloudTrail données, et autorisez les deux `int` et les nombres `float` formatés. Pour de meilleurs résultats, utilisez la version 1.4.0 ou supérieure de la bibliothèque de CloudTrail traitement.

L'exemple d'extrait suivant montre un numéro formaté `float`, `2.0`, pour le paramètre `desiredCount` dans le bloc `ResponseParameters` d'un événement de données.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

L'exemple d'extrait suivant montre un numéro formaté `int`, 2, pour le paramètre `desiredCount` dans le bloc `ResponseParameters` d'un événement de données.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

Rapports d'avancement

Implémentez l'`ProgressReporter`interface pour personnaliser les rapports sur la progression de la bibliothèque de CloudTrail traitement. `ProgressReporter`déclare deux méthodes : `reportStart()` et`reportEnd()`, qui sont appelées au début et à la fin des opérations suivantes :

- Interrogation des messages provenant d'Amazon SQS
- Analyse des messages provenant d'Amazon SQS
- Traitement d'une source Amazon SQS pour les journaux CloudTrail

- Suppression des messages provenant d'Amazon SQS
- Téléchargement d'un fichier CloudTrail journal
- Traitement d'un fichier CloudTrail journal

Ces deux méthodes reçoivent un objet `ProgressStatus` qui contient des informations sur l'opération exécutée. Le membre `progressState` contient un membre de l'énumération `ProgressState` qui identifie l'opération en cours. Ce membre peut contenir des informations supplémentaires dans le membre `progressInfo`. En outre, tout objet que vous renvoyez à partir de `reportStart()` est transmis à `reportEnd()`, de sorte que vous puissiez fournir des informations contextuelles, telles que l'heure de début du traitement de l'événement.

Voici un exemple d'implémentation qui fournit des informations concernant la durée d'une opération :

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

Si vous n'implémentez pas votre propre interface `ProgressReporter`, l'objet `DefaultExceptionHandler`, qui affiche le nom de l'état en cours d'exécution, est utilisé à la place.

Gestion des erreurs

L'interface `ExceptionHandler` vous permet de fournir un traitement spécial lorsqu'une exception se produit pendant le traitement des journaux. `ExceptionHandler` déclare une méthode de rappel unique, `handleException()`, qui reçoit un objet `ProcessingLibraryException` avec un contexte concernant l'exception qui s'est produite.

Vous pouvez utiliser la méthode `getStatus()` de l'objet `ProcessingLibraryException` transmis pour découvrir l'opération qui était en cours d'exécution lorsque l'exception s'est produite et obtenir des informations supplémentaires sur l'état de l'opération. L'objet `ProcessingLibraryException` est dérivé de la classe `Exception` standard de Java ; vous pouvez donc également récupérer des informations sur l'exception en appelant l'une des méthodes d'exception.

Voir l'exemple d'implémentation suivant :

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

Si vous ne fournissez pas votre propre interface `ExceptionHandler`, l'objet `DefaultExceptionHandler`, qui affiche un message d'erreur standard, sera utilisé à la place.

> **Note**
>
> Si le `deleteMessageUponFailure` paramètre est défini comme tel`true`, la bibliothèque de CloudTrail traitement ne fait pas la distinction entre les exceptions générales et les erreurs de traitement et peut supprimer les messages de file d'attente.
>
> 1. Vous utilisez par exemple le `SourceFilter` pour filtrer les messages par horodatage.
> 2. Toutefois, vous ne disposez pas des autorisations requises pour accéder au compartiment S3 qui reçoit les fichiers CloudTrail journaux. Etant donné que vous n'avez pas les autorisations requises, une `AmazonServiceException` est renvoyée. La bibliothèque CloudTrail de traitement l'intègre dans un `CallBackException` fichier.
> 3. L'objet `DefaultExceptionHandler` journalise cela comme une erreur, mais ne permet pas d'identifier la cause première, à savoir que vous n'avez pas les autorisations

requises. La bibliothèque CloudTrail de traitement considère qu'il s'agit d'une erreur de traitement et supprime le message, même s'il contient un fichier CloudTrail journal valide.

Si vous souhaitez filtrer les messages avec `SourceFilter`, vérifiez que votre service `ExceptionHandler` peut faire la distinction entre les exceptions et les erreurs de traitement.

Ressources supplémentaires

Pour plus d'informations sur la bibliothèque CloudTrail de traitement, consultez les rubriques suivantes :

- CloudTrail GitHub Projet Processing Library, qui inclut un exemple de code illustrant comment implémenter une application CloudTrail Processing Library.
- CloudTrail Documentation du package Java de la bibliothèque de traitement.

Sécurité dans AWS CloudTrail

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

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

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

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation CloudTrail. Les rubriques suivantes expliquent comment procéder à la configuration CloudTrail pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos CloudTrail ressources.

Rubriques

Protection des données dans AWS CloudTrail

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS CloudTrail. 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 Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

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

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec CloudTrail ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI 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 une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Par défaut, les fichiers journaux d' CloudTrail événements sont chiffrés à l'aide du chiffrement côté serveur (SSE) Amazon S3. Vous pouvez également choisir de chiffrer vos fichiers journaux avec une clé AWS Key Management Service (AWS KMS). Vous pouvez stocker vos fichiers journaux dans votre compartiment aussi longtemps que vous le souhaitez. Vous pouvez également définir des règles de cycle de vie d'Amazon S3 pour archiver ou supprimer les fichiers journaux automatiquement. Si vous souhaitez recevoir des notifications lors de la transmission et de la validation des fichiers journaux, vous pouvez configurer des notifications Amazon SNS.

Les meilleures pratiques de sécurité suivantes concernent également la protection des données dans CloudTrail :

- Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS)
- Politique relative aux compartiments Amazon S3 pour CloudTrail
- Validation de l' CloudTrail intégrité du fichier journal
- Partage de fichiers CloudTrail journaux entre AWS comptes

Les fichiers CloudTrail journaux étant stockés dans un ou plusieurs compartiments dans Amazon S3, vous devez également consulter les informations relatives à la protection des données dans le guide de l'utilisateur d'Amazon Simple Storage Service. Pour plus d'informations, consultez la section Protection des données dans Amazon S3.

Identity and Access Management pour AWS CloudTrail

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser CloudTrail les ressources. IAM est 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 AWS CloudTrail fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour AWS CloudTrail
- AWS CloudTrail exemples de politiques basées sur les ressources
- Politique relative aux compartiments Amazon S3 pour CloudTrail
- Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake
- Politique relative aux rubriques Amazon SNS pour CloudTrail
- Résolution des problèmes AWS CloudTrail d'identité et d'accès
- Utilisation de rôles liés à un service pour AWS CloudTrail
- AWS politiques gérées pour AWS CloudTrail

Public ciblé

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

Utilisateur du service : si vous utilisez le CloudTrail service 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 nouvelles CloudTrail fonctionnalités 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 CloudTrail, consultezRésolution des problèmes AWS CloudTrail d'identité et d'accès.

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

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

Authentification par des identités

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

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

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

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

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

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 vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

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

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations

pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

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

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

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

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

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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

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

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

Politiques basées sur l'identité

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

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

une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

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

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

Listes de contrôle d'accès (ACL)

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

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

Autres types de politique

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

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour

une entité. Les autorisations 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 remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous 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 politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

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

Comment AWS CloudTrail fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à CloudTrail, découvrez les fonctionnalités IAM disponibles. CloudTrail

Fonctionnalités IAM que vous pouvez utiliser avec AWS CloudTrail

Fonction IAM	CloudTrail soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Partielle
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Non
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont CloudTrail les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour CloudTrail

Prend en charge les politiques basées sur l'identité	Oui

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

ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour CloudTrail

Pour consulter des exemples de politiques CloudTrail basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS CloudTrail

Politiques basées sur les ressources au sein de CloudTrail

Prend en charge les politiques basées sur les ressources	Partielle

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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources

accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

CloudTrail prend en charge les politiques basées sur les ressources sur les canaux utilisés pour les intégrations de CloudTrail Lake avec des sources d'événements extérieures à. AWS La politique basée sur les ressources pour le canal définit quelles entités principales (comptes, utilisateurs, rôles et utilisateurs fédérés) peuvent appeler `PutAuditEvents` sur le canal pour transmettre des événements sur le stockage de données d'événement. Pour plus d'informations sur la création d'intégrations avec CloudTrail Lake, consultezCréez une intégration avec une source d'événements en dehors de AWS.

Exemples

Pour consulter des exemples de politiques CloudTrail basées sur les ressources, consultez. AWS CloudTrail exemples de politiques basées sur les ressources

Actions politiques pour CloudTrail

Prend en charge les actions de politique	Oui

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

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

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

Pour consulter la liste des CloudTrail actions, reportez-vous à la section Actions définies par AWS CloudTrail dans la référence d'autorisation de service.

Les actions de politique en CloudTrail cours utilisent le préfixe suivant avant l'action :

```
cloudtrail
```

Par exemple, pour accorder à une personne l'autorisation de répertorier des identifications pour un journal de suivi à l'aide `ListTags` de l'opération d'API, vous incluez l'action `cloudtrail:ListTags` dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. CloudTrail définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

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

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
      "cloudtrail:RemoveTags
```

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

```
"Action": "cloudtrail:Get*"
```

Ressources politiques pour CloudTrail

Prend en charge les ressources de politique	Oui

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

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

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

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

Pour consulter la liste des types de CloudTrail ressources et de leurs ARN, consultez la section Ressources définies par AWS CloudTrail dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS CloudTrail.

Il existe trois types de ressources : les sentiers, les magasins de données sur les événements et les canaux. CloudTrail Chaque ressource possède un Amazon Resource Name (ARN) unique qui lui est associé. Dans une stratégie, vous utilisez un ARN pour identifier la ressource à laquelle la politique s'applique. CloudTrail ne prend actuellement pas en charge d'autres types de ressources, parfois appelés sous-ressources.

La CloudTrail ressource de suivi possède l'ARN suivant :

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

La ressource de banque de données d' CloudTrail événements possède l'ARN suivant :

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

La ressource du CloudTrail canal possède l'ARN suivant :

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

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

Par exemple, pour un fichier Compte AWS portant l'ID *123456789012*, pour spécifier un parcours nommé *My-Trail* qui existe dans la région USA Est (Ohio) dans votre relevé, utilisez l'ARN suivant :

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

Pour spécifier tous les sentiers appartenant à un compte spécifique Région AWS, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

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

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

De nombreuses actions d' CloudTrail API impliquent plusieurs ressources. Par exemple, `CreateTrail` nécessite un compartiment Amazon S3 pour stocker les fichiers journaux, de sorte qu'un utilisateur doit disposer des autorisations pour écrire dans le compartiment. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

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

Clés de conditions de politique pour CloudTrail

Prend en charge les clés de condition de politique spécifiques au service	Non

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

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

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

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

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

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

CloudTrail ne définit pas ses propres clés de condition, mais il prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de CloudTrail condition, reportez-vous à la section Clés de condition pour AWS CloudTrail la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par AWS CloudTrail.

ACL dans CloudTrail

Prend en charge les listes ACL	Non

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

ABAC avec CloudTrail

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources.

L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Bien que vous puissiez associer des balises aux CloudTrail ressources, elle CloudTrail ne permet de contrôler l'accès aux magasins de données d'événements et aux canaux de CloudTrail Lake qu'en fonction des balises. Vous ne pouvez pas contrôler l'accès aux journaux d'activité en fonction des identifications.

Vous pouvez associer des balises aux CloudTrail ressources ou transmettre des balises dans une demande à CloudTrail. Pour plus d'informations sur le balisage des CloudTrail ressources, reportez-vous aux sections Création d'un journal de suivi etCréation, mise à jour et gestion de sentiers à l'aide du AWS CLI.

Utilisation d'informations d'identification temporaires avec CloudTrail

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour CloudTrail

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour CloudTrail

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM.

Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber CloudTrail les fonctionnalités. Modifiez les rôles de service uniquement lorsque CloudTrail vous recevez des instructions à cet effet.

Rôles liés à un service pour CloudTrail

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

CloudTrail prend en charge un rôle lié à un service pour l'intégration avec. AWS Organizations Ce rôle est obligatoire pour la création d'un journal de suivi ou d'un entrepôt de données d'événement d'organisation. Les traces des organisations et les stockages de données sur les événements enregistrent les événements pour tous Comptes AWS les membres d'une organisation. Pour plus d'informations sur la création ou la gestion de rôles CloudTrail liés à un service, consultez. Utilisation de rôles liés à un service pour AWS CloudTrail

Exemples de politiques basées sur l'identité pour AWS CloudTrail

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier CloudTrail des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par CloudTrail, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS CloudTrail dans la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer CloudTrail des ressources 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 politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

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

CloudTrail ne possède pas de clés de contexte spécifiques au service que vous pouvez utiliser dans l'`Condition`élément des déclarations de politique.

Exemple : autoriser et refuser des actions pour un journal de suivi spécifié

L'exemple suivant illustre une politique qui permet aux utilisateurs de cette politique d'afficher l'état et la configuration d'un journal de suivi et de démarrer et d'arrêter la journalisation pour un journal de suivi nommé *`My-First-Trail`*. Ce sentier a été créé dans la région USA Est (Ohio) (sa région d'origine) Compte AWS avec l'ID *`123456789012`*.

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

```
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
            ]
        }
    ]
}
```

L'exemple suivant illustre une politique qui refuse explicitement les CloudTrail actions pour toute piste non nommée *My-First-Trail*.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

Exemples : créer et appliquer des politiques pour des actions sur des journaux de suivi spécifiques

Vous pouvez utiliser les autorisations et les politiques pour contrôler la capacité d'un utilisateur à effectuer des actions spécifiques sur les CloudTrail sentiers.

Par exemple, vous ne voulez pas que les utilisateurs du groupe de développeurs de votre entreprise démarrent ou arrêtent la journalisation sur un journal de suivi spécifique. Toutefois, vous souhaiterez peut-être leur accorder l'autorisation d'effectuer les actions `DescribeTrails` et `GetTrailStatus`

sur le journal de suivi. Vous voulez que les utilisateurs du groupe de développeurs effectuent les actions `StartLogging` ou `StopLogging` sur les journaux de suivi qu'ils gèrent.

Vous pouvez créer deux déclarations de politique et les attacher au groupe de développeurs créé dans IAM. Pour plus d'informations sur les groupes dans IAM, consultez Groupes IAM dans le Guide de l'utilisateur IAM.

Dans la première politique, vous rejetez les actions `StartLogging` et `StopLogging` pour l'ARN du journal d'activité que vous spécifiez. Dans l'exemple suivant, l'ARN du suivi est `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

Dans la deuxième politique, les `GetTrailStatus` actions `DescribeTrails` et sont autorisées sur toutes les CloudTrail ressources :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
```

```
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Si un utilisateur du groupe de développeurs tente de démarrer ou d'arrêter la journalisation sur le journal d'activité que vous avez spécifié dans la première politique, cet utilisateur reçoit une exception de refus d'accès. Les utilisateurs du groupe de développeurs peuvent commencer et arrêter la journalisation des journaux de suivi qu'ils créent et gèrent.

Les exemples suivants montrent que le groupe de développeurs est configuré dans un AWS CLI profil nommé`devgroup`. Tout d'abord, un utilisateur de `devgroup` exécute la commande `describe-trails`.

```
$ aws --profile devgroup cloudtrail describe-trails
```

La commande s'est terminée avec succès avec la sortie suivante :

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
            "S3BucketName": "myS3bucket ",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

L'utilisateur exécute ensuite la commande `get-trail-status` sur le journal de suivi que vous avez spécifié dans la première politique.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

La commande s'est terminée avec succès avec la sortie suivante :

```
{
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

Ensuite, un utilisateur de `devgroup` exécute la commande `stop-logging` sur le même journal de suivi.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

La commande renvoie une exception d'accès rejeté, telle que la suivante :

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

L'utilisateur exécute la commande `start-logging` sur le même suivi.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

La commande renvoie une fois de plus une exception d'accès rejeté, telle que la suivante :

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

Exemples : rejeter l'accès à la création ou à la suppression de magasins de données d'événement en fonction des identifications

Dans l'exemple de politique suivant, l'autorisation de créer un entrepôt de données d'événement avec `CreateEventDataStore` est refusée si au moins l'une des conditions suivantes n'est pas remplie :

- L'entrepôt de données d'événement ne s'est pas vu appliquer la clé de balise `stage`.
- La valeur de la balise stage n'est pas `alpha`, `beta`, `gamma`, ou `prod`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

Dans l'exemple de politique suivant, l'autorisation de supprimer un entrepôt de données d'événement avec `DeleteEventDataStore` est refusée si l'entrepôt de données d'événement a une balise `stage` dont la valeur est `prod`. Une politique comme celle-ci peut aider à protéger un entrepôt de données d'événement contre la suppression accidentelle.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

Utilisation de la console CloudTrail

Pour accéder à la AWS CloudTrail console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails CloudTrail des ressources de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

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

Octroi d'autorisations pour CloudTrail l'administration

Pour permettre aux rôles ou aux utilisateurs IAM d'administrer une CloudTrail ressource, telle qu'un parcours, un magasin de données d'événements ou un canal, vous devez accorder des autorisations explicites pour effectuer les actions associées aux CloudTrail tâches. Dans la plupart des cas, vous pouvez utiliser une politique AWS gérée contenant des autorisations prédéfinies.

> **Note**
>
> Les autorisations que vous accordez aux utilisateurs pour effectuer des tâches d' CloudTrail administration ne sont pas les mêmes que CloudTrail celles requises pour envoyer des fichiers journaux dans des compartiments Amazon S3 ou envoyer des notifications aux rubriques Amazon SNS. Pour plus d'informations sur ces autorisations, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.
> Si vous configurez l'intégration avec Amazon CloudWatch Logs, cela nécessite CloudTrail également un rôle que celui-ci peut assumer pour transmettre des événements à un groupe de CloudWatch journaux Amazon Logs. Vous devez créer le rôle qui CloudTrail utilise. Pour plus d'informations, consultez Octroi de l'autorisation d'afficher et de configurer CloudWatch

les informations Amazon Logs sur la CloudTrail console et Envoyer des événements à CloudWatch Logs.

Les politiques AWS gérées suivantes sont disponibles pour CloudTrail :

- AWSCloudTrail_FullAccess— Cette politique fournit un accès complet aux CloudTrail actions sur les CloudTrail ressources, telles que les sentiers, les magasins de données sur les événements et les canaux. Cette politique fournit les autorisations requises pour créer, mettre à jour et supprimer des CloudTrail traces, des banques de données d'événements et des chaînes.

  Cette politique fournit également des autorisations pour gérer le compartiment Amazon S3, le groupe de CloudWatch journaux pour les journaux et une rubrique Amazon SNS pour un suivi. Cependant, la politique `AWSCloudTrail_FullAccess` gérée n'autorise pas la suppression du compartiment Amazon S3, du groupe de CloudWatch journaux pour les journaux ou d'une rubrique Amazon SNS. Pour plus d'informations sur les politiques gérées pour les autres Services AWS, consultez le Guide de référence des politiques AWS gérées.

  > **Note**
  >
  > La AWSCloudTrail_FullAccesspolitique n'est pas destinée à être largement partagée entre vous Compte AWS. Les utilisateurs ayant ce rôle peuvent désactiver ou reconfigurer les fonctions d'audit les plus sensibles et les plus importantes dans leur Comptes AWS. Pour cette raison, vous ne devez appliquer cette politique qu'aux administrateurs de compte. Vous devez contrôler et surveiller étroitement l'utilisation de cette politique.

- AWSCloudTrail_ReadOnlyAccess— Cette politique accorde des autorisations pour consulter la CloudTrail console, y compris les événements récents et l'historique des événements. Cette politique vous permet également de consulter les journaux de suivi, les entrepôts de données d'événement et les canaux existants. Les rôles et les utilisateurs soumis à cette politique peuvent télécharger l'historique des événements, mais ils ne peuvent pas créer ou mettre à jour des journaux de suivi, des entrepôts de données d'événement ou des canaux.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Ressources supplémentaires

Pour en savoir plus sur l'utilisation d'IAM pour donner aux identités, telles que les utilisateurs et les rôles, l'accès aux ressources de votre compte, consultez les sections Configuration de l'IAM et gestion des accès aux AWS ressources dans le Guide de l'utilisateur IAM.

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

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

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

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

Octroi d'autorisations personnalisées aux CloudTrail utilisateurs

CloudTrail les politiques accordent des autorisations aux utilisateurs qui travaillent avec CloudTrail. Si vous devez accorder des autorisations différentes aux utilisateurs, vous pouvez associer une CloudTrail politique à un groupe IAM ou à un utilisateur. Vous pouvez modifier la politique de sorte à inclure ou exclure des autorisations spécifiques. Vous pouvez également créer votre propre politique personnalisée. Les politiques sont des documents JSON qui définissent les actions qu'un utilisateur est autorisé à effectuer, ainsi que les ressources sur lesquelles il est autorisé à effectuer ces actions. Pour plus d'exemples, consultez Exemple : autoriser et refuser des actions pour un journal de suivi spécifié et Exemples : créer et appliquer des politiques pour des actions sur des journaux de suivi spécifiques.

Table des matières

- Octroi de l'autorisation d'afficher et de configurer CloudWatch les informations Amazon Logs sur la CloudTrail console
- Informations supplémentaires

Accès en lecture seule

L'exemple suivant montre une politique qui accorde un accès en lecture seule aux CloudTrail sentiers. Cela équivaut à la politique gérée AWSCloudTrail_ReadOnlyAccess. Elle accorde aux utilisateurs l'autorisation de consulter les informations des journaux de suivi, mais pas de créer ou de mettre à jour des journaux de suivi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:Get*",
                "cloudtrail:Describe*",
                "cloudtrail:List*",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

Dans les déclarations de politique, l'élément `Effect` spécifie si les actions sont autorisées ou refusées. L'élément `Action` répertorie les actions spécifiques que l'utilisateur est autorisé à effectuer. L'`Resource`élément répertorie les AWS ressources sur lesquelles l'utilisateur est autorisé à effectuer ces actions. Pour les politiques qui contrôlent l'accès aux CloudTrail actions, l'`Resource`élément est généralement défini sur * un caractère générique qui signifie « toutes les ressources ».

Les valeurs dans l'élément `Action` correspondent aux API prises en charge par les services. Les actions sont `cloudtrail:` précédées de ce qui indique qu'elles font référence à CloudTrail des actions. Vous pouvez utiliser le caractère générique * dans l'élément `Action`, comme dans les exemples suivants :

- `"Action": ["cloudtrail:*Logging"]`

Cela permet toutes les CloudTrail actions qui se terminent par « Logging » (`StartLogging`,`StopLogging`).

- `"Action": ["cloudtrail:*"]`

  Cela permet toutes les CloudTrail actions, mais pas les actions pour les autres AWS services.

- `"Action": ["*"]`

  Cela permet toutes les AWS actions. Cette autorisation convient pour un utilisateur qui agit en tant qu'administrateur AWS pour votre compte.

La politique en lecture seule n'accorde pas l'autorisation à l'utilisateur pour les `CreateTrail`, `UpdateTrail`, `StartLogging` et `StopLogging` actions. Utilisateurs avec cette politique ne sont pas autorisés à créer des journaux de suivi, mettre à jour des journaux de suivi ou activer et désactiver la journalisation. Pour la liste des CloudTrail actions, consultez la référence de AWS CloudTrail l'API.

Accès complet à

L'exemple suivant montre une politique qui accorde un accès complet à CloudTrail. Cela équivaut à la politique gérée AWSCloudTrail_FullAccess. Il accorde aux utilisateurs l'autorisation d'effectuer toutes les CloudTrail actions. Il permet également aux utilisateurs de consigner les événements liés aux données dans Amazon S3 et AWS Lambda de gérer des fichiers dans des compartiments Amazon S3, de gérer la manière dont CloudWatch Logs surveille les événements de CloudTrail journal et de gérer les rubriques Amazon SNS dans le compte auquel l'utilisateur est associé.

> **Important**
>
> La AWSCloudTrail_FullAccesspolitique ou les autorisations équivalentes ne sont pas destinées à être largement partagées sur l'ensemble de votre AWS compte. Les utilisateurs dotés de ce rôle ou d'un accès équivalent ont la possibilité de désactiver ou de reconfigurer les fonctions d'audit les plus sensibles et les plus importantes de leurs AWS comptes. Pour cette raison, cette politique doit être appliquée uniquement aux administrateurs de compte, et l'utilisation de cette politique doit être étroitement contrôlée et surveillée.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Octroi de l'autorisation AWS Config d'afficher les informations sur la CloudTrail console

Vous pouvez consulter les informations relatives aux événements sur la CloudTrail console, y compris les ressources associées à cet événement. Pour ces ressources, vous pouvez choisir l' AWS Config icône pour afficher la chronologie de cette ressource dans la AWS Config console. Associez cette politique à vos utilisateurs pour leur accorder un accès en lecture seule AWS Config . La politique ne leur accorde pas l'autorisation de modifier les paramètres dans AWS Config.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

Pour plus d'informations, consultez Affichage des ressources référencées avec AWS Config.

Octroi de l'autorisation d'afficher et de configurer CloudWatch les informations Amazon Logs sur la CloudTrail console

Vous pouvez consulter et configurer l'envoi d'événements à CloudWatch Logs dans la CloudTrail console si vous disposez des autorisations suffisantes. Il s'agit d'autorisations qui peuvent aller au-

delà de celles accordées aux CloudTrail administrateurs. Associez cette politique aux administrateurs qui configureront et géreront CloudTrail l'intégration avec CloudWatch Logs. La politique ne leur accorde pas d'autorisations directement dans CloudTrail ou dans les CloudWatch journaux, mais accorde plutôt les autorisations nécessaires pour créer et configurer le rôle qu'ils CloudTrail assumeront pour transmettre correctement les événements à votre groupe de CloudWatch journaux.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

Pour plus d'informations, consultez Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.

Informations supplémentaires

Pour en savoir plus sur l'utilisation d'IAM pour donner aux identités, telles que les utilisateurs et les rôles, l'accès aux ressources de votre compte, consultez les sections Mise en route et Gestion de l'accès aux AWS ressources dans le Guide de l'utilisateur IAM.

AWS CloudTrail exemples de politiques basées sur les ressources

CloudTrail prend en charge les politiques d'autorisation basées sur les ressources pour les CloudTrail canaux utilisés pour les intégrations de CloudTrail Lake. Pour plus d'informations sur la création d'intégrations avec CloudTrail Lake, consultezCréez une intégration avec une source d'événements en dehors de AWS.

Les informations requises pour la politique sont déterminées par le type d'intégration.

- Pour une intégration des directions, CloudTrail la politique doit contenir les Compte AWS identifiants du partenaire et vous oblige à saisir l'identifiant externe unique fourni par le partenaire. CloudTrail ajoute automatiquement les Compte AWS identifiants du partenaire à la politique de ressources lorsque vous créez une intégration à l'aide de la CloudTrail console. Reportez-vous à la documentation du partenaire pour savoir comment obtenir les Compte AWS numéros requis pour la politique.
- Pour une intégration de solution, vous devez spécifier au moins un Compte AWS identifiant comme identifiant principal, et vous pouvez éventuellement saisir un identifiant externe pour éviter toute confusion entre les adjoints.

Voici les conditions requises pour la politique basée sur les ressources :

- L'ARN de ressource défini dans la politique doit correspondre à l'ARN du canal auquel la politique est attachée.
- La politique ne contient qu'une seule action : `cloudtrail-data:PutAuditEvents`
- La politique contient au moins une instruction. La politique peut comporter un maximum de 20 instructions.
- Chaque instruction comprend au moins un principal. Une instruction peut comporter un maximum de 50 principaux.

Le propriétaire du canal peut appeler l'API `PutAuditEvents` sur celui-ci à moins que la politique ne lui refuse l'accès à la ressource.

Rubriques

- Exemple : fournir un accès au canal aux principaux
- Exemple : utilisation d'un ID externe afin d'éviter tout problème d'adjoint confus

Exemple : fournir un accès au canal aux principaux

L'exemple suivant accorde des autorisations aux principaux avec les ARN et leur `arn:aws:iam::111122223333:root` permet `arn:aws:iam::444455556666:root` d'`arn:aws:iam::123456789012:root`appeler l'PutAuditEventsAPI sur le CloudTrail canal avec l'ARN. `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Exemple : utilisation d'un ID externe afin d'éviter tout problème d'adjoint confus

L'exemple suivant utilise un ID externe afin d'éviter tout problème d'adjoint confus. Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire.

Le partenaire d'intégration crée l'ID externe à utiliser dans la politique. Il vous fournit ensuite l'ID externe pour la création de l'intégration. Cette valeur peut être n'importe quelle chaîne unique, telle qu'une phrase de passe ou un numéro de compte.

L'exemple accorde des autorisations aux principaux avec les ARN et `arn:aws:iam::111122223333:root` permet d'`arn:aws:iam::123456789012:root`appeler l'PutAuditEventsAPI sur la ressource du CloudTrail canal si l'appel à l'`PutAuditEvents`API inclut la valeur d'ID externe définie dans la politique. `arn:aws:iam::444455556666:root`

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

```
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "uniquePartnerExternalID"
                }
            }
        }
    ]
}
```

Politique relative aux compartiments Amazon S3 pour CloudTrail

Par défaut, les objets et les compartiments Amazon S3 sont privés. Seul le propriétaire de la ressource (le compte AWS qui a créé le compartiment) peut accéder au compartiment et aux objets qu'il contient. Le propriétaire de la ressource peut accorder des autorisations d'accès à d'autres ressources et à d'autres utilisateurs en créant une stratégie d'accès.

Si vous souhaitez créer ou modifier un compartiment Amazon S3 pour recevoir les fichiers journaux pour le journal d'activité d'une organisation, vous devez modifier la politique de compartiment. Pour plus d'informations, consultez Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface.

Pour fournir des fichiers journaux à un compartiment S3, vous CloudTrail devez disposer des autorisations requises, et celui-ci ne peut pas être configuré en tant que compartiment Requester Pays.

CloudTrail ajoute les champs suivants dans la politique pour vous :

- Les SID autorisés
- Le nom du compartiment
- Le nom principal du service pour CloudTrail
- Le nom du dossier dans lequel les fichiers journaux sont stockés, y compris le nom du compartiment, un préfixe (si vous en avez spécifié un) et votre identifiant de AWS compte

Comme bonne pratique en matière de sécurité, ajoutez une clé de condition `aws:SourceArn` à la politique de compartiment Amazon S3. La clé de condition globale IAM `aws:SourceArn` permet de garantir que les CloudTrail écritures dans le compartiment S3 ne concernent qu'un ou plusieurs sentiers spécifiques. La valeur de `aws:SourceArn` est toujours l'ARN du journal d'activité (ou de la série d'ARN du journal d'activité) qui utilise le compartiment pour stocker les journaux. Assurez-vous d'ajouter la `aws:SourceArn` clé de condition aux stratégies de compartiment S3 pour les suivis existants.

La politique suivante permet d' CloudTrail écrire des fichiers journaux dans le compartiment à partir de fichiers pris en charge Régions AWS. Remplacez *myBucketName[OptionalPrefix]/*, *MyAccountId*, *region* et *TrailName* par les valeurs appropriées à votre configuration.

Politique de compartiment S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
```

```
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur Régions AWS, voirCloudTrail Régions prises en charge.

Table des matières

Spécification d'un compartiment existant pour la livraison du CloudTrail journal

Si vous avez spécifié un compartiment S3 existant comme emplacement de stockage pour la livraison des fichiers journaux, vous devez associer au compartiment une politique autorisant CloudTrail l'écriture dans le compartiment.

> **Note**
>
> Il est recommandé d'utiliser un compartiment S3 dédié pour les CloudTrail journaux.

Pour ajouter la CloudTrail politique requise à un compartiment Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez le compartiment dans lequel vous CloudTrail souhaitez envoyer vos fichiers journaux, puis choisissez Permissions.
3. Choisissez Modifier.
4. Copiez la S3 bucket policy dans la fenêtre Éditeur de politique de compartiment. Remplacez les espaces réservés en italique par les noms du compartiment, le préfixe et le numéro de compte. Si vous avez spécifié un préfixe lorsque vous avez créé votre journal d'activité, incluez-le ici. Le préfixe est un ajout facultatif à la clé d'objet S3 qui crée une organisation de type dossier dans le compartiment.

> **Note**
>
> Si une ou plusieurs politiques sont déjà associées au bucket existant, ajoutez les instructions pour CloudTrail accéder à cette ou ces politiques. Évaluez le jeu d'autorisations obtenu pour vérifier son adéquation pour les utilisateurs appelés à accéder au compartiment.

Réception des fichiers journaux depuis d'autres comptes

Vous pouvez configurer CloudTrail pour transférer les fichiers journaux de plusieurs AWS comptes vers un seul compartiment S3. Pour plus d'informations, consultez Réception de fichiers CloudTrail journaux provenant de plusieurs comptes.

Créez ou mettez à jour un compartiment Amazon S3 pour stocker les fichiers journaux du journal d'activité d'une organisation

Vous devez spécifier un compartiment Amazon S3 pour recevoir les fichiers journaux pour un journal d'activité d'une organisation. Ce compartiment doit disposer d'une politique CloudTrail permettant d'y placer les fichiers journaux de l'organisation.

Voici un exemple de politique pour un compartiment Amazon S3 nommé *myOrganizationBucket*, qui appartient au compte de gestion de l'organisation. Remplacez *myOrganizationBucket*, *region*, *ManagementAccountID*, *TrailName* et *O-OrganizationID par les valeurs de votre organisation*

Cette politique de compartiment contient trois instructions.

- La première instruction permet CloudTrail d'appeler l'`GetBucketAcl`action Amazon S3 sur le compartiment Amazon S3.
- La seconde instruction permet de se connecter dans le cas où le suivi est modifié d'un suivi d'organisation à un suivi pour ce compte uniquement.
- La troisième instruction autorise la journalisation pour le suivi d'organisation.

L'exemple de politique inclut une clé de condition `aws:SourceArn` de la politique de compartiment Amazon S3. La clé de condition globale IAM `aws:SourceArn` permet de garantir que les CloudTrail écritures dans le compartiment S3 ne concernent qu'un ou plusieurs sentiers spécifiques. Dans un journal de suivi de l'organisation, la valeur de `aws:SourceArn` doit être un ARN de suivi appartenant au compte de gestion qui utilise l'ID du compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Cet exemple de politique n'autorise pas tous les utilisateurs des comptes membres à accéder aux fichiers journaux créés pour l'organisation. Par défaut, les fichiers journaux de l'organisation sont accessibles uniquement au compte de gestion. Pour plus d'informations sur la manière d'autoriser un accès en lecture au compartiment Amazon S3 pour les utilisateurs IAM des comptes membres, consultez Partage de fichiers CloudTrail journaux entre AWS comptes.

Résolution des erreurs de politique de compartiment Amazon S3

Les sections suivantes décrivent la résolution des problèmes liés à la politique de compartiment S3.

Erreurs courantes de configuration de politique Amazon S3

Lorsque vous créez un nouveau bucket dans le cadre de la création ou de la mise à jour d'un trail CloudTrail, vous associez les autorisations requises à votre bucket. La politique de compartiment utilise le nom principal du service`"cloudtrail.amazonaws.com"`, qui permet CloudTrail de fournir des journaux pour toutes les régions.

CloudTrail S'il ne fournit pas de journaux pour une région, il est possible que votre compartiment dispose d'une ancienne politique qui spécifie les identifiants de CloudTrail compte pour chaque région. Cette politique donne CloudTrail l'autorisation de fournir des journaux uniquement pour les régions spécifiées.

Il est recommandé de mettre à jour la politique pour utiliser une autorisation auprès du directeur du CloudTrail service. Pour cela, remplacez les ARN de l'ID de compte par le nom principal du service : `"cloudtrail.amazonaws.com"`. Cela donne CloudTrail l'autorisation de fournir des journaux pour les régions actuelles et nouvelles. Comme bonne pratique en matière de sécurité, ajoutez une `aws:SourceArn` ou `aws:SourceAccount` clé de condition de la politique de compartiment Amazon S3. Cela permet d'empêcher tout accès non autorisé de compte à votre compartiment S3. Si vous avez déjà des journaux d'activité, veillez à ajouter une ou plusieurs clés de condition. Voici un exemple de configuration de politique recommandée. Remplacez *`myBucketName[OptionalPrefix]/`*, *`MyAccountId`*, *`region`* et *`TrailName`* par les valeurs appropriées à votre configuration.

Example Exemple de politique de compartiment avec le nom principal du service

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
```

```
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Modification d'un préfixe pour un compartiment existant

Si vous essayez d'ajouter, de modifier ou de supprimer un préfixe de fichier journal pour un compartiment S3 qui reçoit les journaux d'un journal d'activité, vous pourriez obtenir l'erreur suivante : Problème avec la politique de compartiment. Une politique de compartiment avec un préfixe incorrect peut empêcher votre journal d'activité de livrer les journaux au compartiment. Pour résoudre ce problème, utilisez la console Amazon S3 pour mettre à jour le préfixe dans la politique de compartiment, puis utilisez la CloudTrail console pour spécifier le même préfixe pour le compartiment dans le journal d'essai.

Pour mettre à jour le préfixe du fichier journal pour un compartiment Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Sélectionnez le compartiment pour lequel vous souhaitez modifier le préfixe, puis choisissez Permissions (Autorisations).
3. Choisissez Modifier.
4. Dans la politique de compartiment, sous `s3:PutObject` l'action, modifiez `Resource` l'entrée pour ajouter, modifier, ou supprimer le *`préfixe`* du fichier journal selon les besoins.

   ```
   "Action": "s3:PutObject",
         "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
   ```

5. Choisissez Save (Enregistrer).

6. Ouvrez la CloudTrail console à l'adresse https://console.aws.amazon.com/cloudtrail/.
7. Choisissez votre journal d'activité et pour Storage location (Emplacement du stockage), cliquez sur l'icône en forme de crayon afin de modifier les paramètres de votre compartiment.
8. Dans S3 bucket (Compartiment S3), choisissez le compartiment dont vous modifiez le préfixe.
9. Dans Log file prefix (Préfixe du fichier journal), mettez à jour le préfixe de manière à refléter le préfixe que vous avez saisi dans la politique de compartiment.
10. Choisissez Save (Enregistrer).

Ressources supplémentaires

Pour plus d'informations sur les compartiments S3 et les politiques, consultez Utilisation des politiques de compartiments (Français non garanti) du Guide de l'utilisateur Amazon Simple Storage Service.

Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake

Par défaut, les objets et les compartiments Amazon S3 sont privés. Seul le propriétaire de la ressource (le compte AWS qui a créé le compartiment) peut accéder au compartiment et aux objets qu'il contient. Le propriétaire de la ressource peut accorder des autorisations d'accès à d'autres ressources et à d'autres utilisateurs en créant une stratégie d'accès.

Pour transmettre les résultats d'une requête CloudTrail Lake à un compartiment S3, vous CloudTrail devez disposer des autorisations requises, et celui-ci ne peut pas être configuré en tant que compartiment Requester Pays.

CloudTrail ajoute les champs suivants dans la politique pour vous :

- Les SID autorisés
- Le nom du compartiment
- Le nom principal du service pour CloudTrail

Comme bonne pratique en matière de sécurité, ajoutez une clé de condition `aws:SourceArn` à la politique de compartiment Amazon S3. La clé de condition globale IAM `aws:SourceArn` permet de garantir que les CloudTrail écritures dans le compartiment S3 ne sont destinées qu'au magasin de données d'événements.

La politique suivante permet de CloudTrail fournir des résultats de requête au bucket à partir de la version prise en charge Régions AWS. Remplacez *myBucketNameMyAccountID* et *myQueryRunningRegion* par les valeurs appropriées à votre configuration. Le *MyAccountID* est l'ID de AWS compte utilisé pour CloudTrail, qui peut être différent de l'ID de AWS compte pour le compartiment S3.

> **Note**
>
> Si votre politique de compartiment inclut une déclaration pour une clé KMS, vous recommandons d'utiliser un ARN de clé KMS totalement qualifié. Si vous utilisez plutôt un alias de clé KMS, AWS KMS la clé est résolue dans le compte du demandeur. En raison de ce comportement, les données peuvent être chiffrées avec une clé KMS qui appartient au demandeur, et non au propriétaire du compartiment.
> S'il s'agit du magasin de données d'événement d'une organisation, vous devez utiliser l'identifiant du compte AWS de gestion. Cela est dû au fait que le compte de gestion conserve la propriété de toutes les ressources de l'organisation.

Politique de compartiment S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
```

```
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

Table des matières

Spécification d'un compartiment existant pour les résultats de la requête CloudTrail Lake

Si vous avez spécifié un compartiment S3 existant comme emplacement de stockage pour la livraison des résultats des requêtes CloudTrail Lake, vous devez attacher une politique au compartiment qui permet de CloudTrail fournir les résultats de la requête au compartiment.

> **Note**
>
> Il est recommandé d'utiliser un compartiment S3 dédié pour les résultats des requêtes CloudTrail Lake.

Pour ajouter la CloudTrail politique requise à un compartiment Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.

2. Choisissez le compartiment dans lequel vous souhaitez CloudTrail envoyer les résultats de votre requête Lake, puis choisissez Permissions.
3. Choisissez Modifier.
4. Copiez la S3 bucket policy for query results dans la fenêtre Éditeur de politique de compartiment. Remplacez les espaces réservés en italique par les noms de votre compartiment, de votre région et de votre ID de compte.

> **Note**
>
> Si une ou plusieurs politiques sont déjà associées au bucket existant, ajoutez les instructions pour CloudTrail accéder à cette ou ces politiques. Évaluez le jeu d'autorisations obtenu pour vérifier son adéquation pour les utilisateurs qui accèdent au compartiment.

Ressources supplémentaires

Pour plus d'informations sur les compartiments S3 et les politiques, consultez Utilisation des politiques de compartiments (Français non garanti) du Guide de l'utilisateur Amazon Simple Storage Service.

Politique relative aux rubriques Amazon SNS pour CloudTrail

Pour envoyer des notifications à une rubrique SNS, vous CloudTrail devez disposer des autorisations requises. CloudTrailattache automatiquement les autorisations requises au sujet lorsque vous créez un sujet Amazon SNS dans le cadre de la création ou de la mise à jour d'un journal dans la CloudTrail console.

> **Important**
>
> Comme bonne pratique de sécurité, pour restreindre l'accès à votre rubrique SNS, nous vous recommandons fortement, après avoir créé ou mis à jour un journal d'activité pour envoyer des notifications SNS, de modifier manuellement la politique IAM attachée à la rubrique SNS pour ajouter des clés de condition. Pour plus d'informations, consultez the section called "Bonnes pratiques de sécurité pour la politique de rubrique SNS" dans cette rubrique.

CloudTrail ajoute pour vous la déclaration suivante à la politique avec les champs suivants :

- Les SID autorisés.
- Le nom principal du service pour CloudTrail.
- La rubrique SNS, avec la région, l'ID de compte et le nom de la rubrique.

La politique suivante permet d' CloudTrail envoyer des notifications concernant la livraison de fichiers journaux depuis les régions prises en charge. Pour plus d'informations, consultez CloudTrail Régions prises en charge. Il s'agit de la politique par défaut attachée à une politique de rubrique SNS nouvelle ou existante lorsque vous créez ou mettez à jour un journal d'activité et que vous choisissez d'activer les notifications SNS.

Politique de rubrique SNS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
        }
    ]
}
```

Pour utiliser une rubrique Amazon SNS AWS KMS chiffrée pour envoyer des notifications, vous devez également activer la compatibilité entre la source de l'événement CloudTrail () et la rubrique cryptée en ajoutant l'instruction suivante à la politique du. AWS KMS key

Politique de clé KMS

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

```
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations, voir Activer la compatibilité entre les sources d'événements provenant AWS des services et des rubriques cryptées.

Table des matières

Bonnes pratiques de sécurité pour la politique de rubrique SNS

Par défaut, la déclaration de politique IAM CloudTrail attachée à votre rubrique Amazon SNS autorise CloudTrail le principal du service à publier sur une rubrique SNS, identifiée par un ARN. Pour empêcher un attaquant d'accéder à votre rubrique SNS et d'envoyer des notifications au nom des destinataires de la CloudTrail rubrique, modifiez manuellement votre politique de rubrique CloudTrail SNS pour ajouter une clé de `aws:SourceArn` condition à la déclaration de politique jointe par. CloudTrail La valeur de cette clé est l'ARN du journal d'activité, ou un tableau d'ARN de piste utilisant la rubrique SNS. Comme elle inclut à la fois l'ID du journal d'activité spécifique et l'ID du compte propriétaire de la piste, elle limite l'accès à la rubrique SNS uniquement aux comptes qui ont l'autorisation de gérer la piste. Avant d'ajouter des clés de condition à votre politique de rubrique SNS, obtenez le nom de la rubrique SNS dans les paramètres de votre journal dans la CloudTrail console.

La clé de condition `aws:SourceAccount` est également prise en charge, mais n'est pas recommandée.

Pour ajouter la clé de condition **`aws:SourceArn`** de votre politique de rubrique SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, sélectionnez Topics (Rubriques).
3. Choisissez la rubrique SNS qui s'affiche dans vos paramètres de piste, puis choisissezModifier.
4. Développez la politique d'accès.
5. Dans Stratégie d'accès Éditeur JSON, recherchez un bloc semblable à l'exemple suivant.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Ajouter un nouveau bloc pour une condition,`aws:SourceArn`Comme illustré dans l'exemple suivant. Pour`aws:SourceArn`est l'ARN de la piste au sujet de laquelle vous envoyez des notifications à SNS.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. Lorsque vous avez terminé de modifier la politique de la rubrique SNS, choisissez Save changes (Enregistrer les modifications).

Pour ajouter la clé de condition **`aws:SourceAccount`** de votre politique de rubrique SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, sélectionnez Topics (Rubriques).
3. Choisissez la rubrique SNS qui s'affiche dans vos paramètres de piste, puis choisissezModifier.
4. Développez la politique d'accès.
5. Dans Stratégie d'accès Éditeur JSON, recherchez un bloc semblable à l'exemple suivant.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Ajouter un nouveau bloc pour une condition,`aws:SourceAccount`Comme illustré dans l'exemple suivant. La valeur de `aws:SourceAccount` est l'identifiant du compte propriétaire du CloudTrail parcours. Cet exemple limite l'accès à la rubrique SNS aux seuls utilisateurs qui peuvent se connecter au AWS compte 123456789012.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
```

```
        }
      }
    }
```

7. Lorsque vous avez terminé les modifications, choisissez Save changes (Enregistrer les modifications).

Spécification d'une rubrique existante pour l'envoi des notifications

Vous pouvez ajouter manuellement les autorisations pour un sujet Amazon SNS à votre politique de sujet dans la console Amazon SNS, puis spécifier le sujet dans la console. CloudTrail

Pour mettre à jour manuellement une politique de rubrique SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Choisissez Rubriques, puis choisissez la rubrique.
3. Choisissez Modifier, puis faites défiler l'écran vers le bas jusqu'à Politique d'accès.
4. Ajoutez le relevé de SNS topic policy avec les valeurs appropriées pour la région, l'ID de compte et le nom du sujet.
5. Si votre sujet est un sujet crypté, vous devez autoriser `kms:GenerateDataKey*` et CloudTrail obtenir les `kms:Decrypt` autorisations nécessaires. Pour plus d'informations, consultez Encrypted SNS topic KMS key policy.
6. Choisissez Enregistrer les modifications.
7. Retournez à la CloudTrail console et spécifiez le sujet du parcours.

Résolution des erreurs de politique de rubrique SNS

Les sections suivantes décrivent la résolution des problèmes liés à la politique de rubrique SNS.

Scénarios

- CloudTrail n'envoie pas de notifications pour une région
- CloudTrail n'envoie pas de notifications pour le compte d'un membre d'une organisation

CloudTrail n'envoie pas de notifications pour une région

Lorsque vous créez un nouveau sujet dans le cadre de la création ou de la mise à jour d'un parcours CloudTrail , associez les autorisations requises à votre sujet. La politique thématique utilise le nom principal du service`"cloudtrail.amazonaws.com"`, qui permet d' CloudTrail envoyer des notifications pour toutes les régions.

S'il ne s' CloudTrail agit pas d'envoyer de notifications pour une région, il est possible que votre sujet ait une ancienne politique qui spécifie les identifiants de CloudTrail compte pour chaque région. Cette politique CloudTrail autorise l'envoi de notifications uniquement pour les régions spécifiées.

La politique thématique suivante permet CloudTrail d'envoyer des notifications uniquement pour les neuf régions spécifiées :

Example politique de rubrique avec ID de compte

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

Cette politique utilise une autorisation basée sur les identifiants de CloudTrail compte individuels. Pour fournir des journaux pour une nouvelle région, vous devez mettre à jour manuellement la politique afin d'inclure l'identifiant de CloudTrail compte de cette région. Par exemple, en raison de l' CloudTrail ajout de la prise en charge de la région USA Est

(Ohio), vous devez mettre à jour la politique pour ajouter l'ID de compte ARN pour cette région :`"arn:aws:iam::475085895292:root"`.

Il est recommandé de mettre à jour la politique pour utiliser une autorisation auprès du directeur du CloudTrail service. Pour cela, remplacez les ARN de l'ID de compte par le nom principal du service : `"cloudtrail.amazonaws.com"`.

Cela donne CloudTrail l'autorisation d'envoyer des notifications pour les régions actuelles et nouvelles. Voici une version mise à jour de la politique précédente :

Example politique de rubrique avec le nom principal du service

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

Vérifiez que la politique comporte les valeurs appropriées :

- Dans le champ `Resource`, spécifiez le numéro de compte du propriétaire de la rubrique. Pour les rubriques que vous créez, spécifiez votre numéro de compte.
- Spécifiez les valeurs appropriées pour la région et le nom de rubrique SNS.

CloudTrail n'envoie pas de notifications pour le compte d'un membre d'une organisation

Lorsqu'un compte membre associé à un historique d' AWS Organizations organisation n'envoie pas de notifications Amazon SNS, il se peut que la configuration de la politique relative aux rubriques SNS pose problème. CloudTrail crée des traces d'organisation dans les comptes des membres même si la validation d'une ressource échoue. Par exemple, la rubrique SNS du journal de l'organisation n'inclut pas tous les identifiants de compte des membres. Si la politique des rubriques SNS est incorrecte, un échec d'autorisation se produit.

Pour vérifier si la politique des rubriques SNS d'un parcours présente un échec d'autorisation, procédez comme suit :

- Depuis la CloudTrail console, consultez la page de détails du parcours. En cas d'échec de l'autorisation, la page de détails inclut un avertissement `SNS authorization failed` et indique qu'il faut corriger la politique des rubriques SNS.
- À partir du AWS CLI, exécutez la get-trail-statuscommande. En cas d'échec de l'autorisation, la sortie de commande inclut le `LastNotificationError` champ avec une valeur de`AuthorizationError`.

Ressources supplémentaires

Pour plus d'informations sur les rubriques SNS et l'abonnement à celles-ci, consultez le Guide du développeur Amazon Simple Notification Service.

Résolution des problèmes AWS CloudTrail d'identité et d'accès

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

Rubriques

- Je ne suis pas autorisé à effectuer une action dans CloudTrail
- Je ne suis pas autorisé à effectuer iam:PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes CloudTrail ressources
- Je ne suis pas autorisé à effectuer iam:PassRole
- Je reçois une exception NoManagementAccountSLRExistsException lorsque j'essaie de créer un journal d'organisation ou un entrepôt de données d'événement

Je ne suis pas autorisé à effectuer une action dans CloudTrail

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `cloudtrail:`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `cloudtrail:`*`GetWidget`*.

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

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'utilisateur `mateojackson` IAM essaie d'utiliser la console pour afficher les détails d'un parcours mais ne dispose pas de la politique CloudTrail gérée appropriée (AWSCloudTrail_FullAccessou AWSCloudTrail_ReadOnlyAccess) ou des autorisations équivalentes appliquées à son compte.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

Dans ce cas, Mateo demande son administrateur de mettre à jour ses politiques pour lui autoriser d'accéder aux informations et au statut du journal de suivi dans la console.

Si vous vous connectez avec un utilisateur ou un rôle IAM doté de la politique AWSCloudTrail_FullAccessgérée ou d'autorisations équivalentes, et que vous ne parvenez pas à configurer AWS Config ou à intégrer Amazon CloudWatch Logs à un journal, il se peut que vous ne disposiez pas des autorisations requises pour l'intégration à ces services. Pour plus d'informations, consultez Octroi de l'autorisation AWS Config d'afficher les informations sur la CloudTrail console et Octroi de l'autorisation d'afficher et de configurer CloudWatch les informations Amazon Logs sur la CloudTrail console.

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 CloudTrail.

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

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans CloudTrail. 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 permettre à des personnes extérieures Compte AWS à moi d'accéder à mes CloudTrail ressources

Vous pouvez créer un rôle et partager CloudTrail des informations entre plusieurs Comptes AWS. Pour plus d'informations, consultez Partage de fichiers CloudTrail journaux entre AWS comptes.

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

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises CloudTrail en charge, consultezComment AWS CloudTrail fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

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 CloudTrail.

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

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans CloudTrail. 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 reçois une exception **`NoManagementAccountSLRExistsException`** lorsque j'essaie de créer un journal d'organisation ou un entrepôt de données d'événement

L'exception `NoManagementAccountSLRExistsException` est levée lorsque le compte de gestion n'a pas de rôle lié à un service. Lorsque vous ajoutez un administrateur délégué à l'aide de l'opération AWS Organizations AWS CLI ou API, le rôle lié au service n'est pas créé s'il n'existe pas.

Lorsque vous utilisez le compte de gestion de votre organisation pour ajouter un administrateur délégué ou créer un historique d'organisation ou un magasin de données d'événements dans la CloudTrail console, ou à l'aide de l' CloudTrailAPI AWS CLI or, vous créez CloudTrail automatiquement un rôle lié à un service pour votre compte de gestion s'il n'en existe pas déjà un.

Si vous n'avez pas ajouté d'administrateur délégué, utilisez la CloudTrail console AWS CLI ou CloudTrail l'API pour ajouter l'administrateur délégué. Pour plus d'informations sur l'ajout d'un administrateur délégué, consultez Ajouter un administrateur CloudTrail délégué et RegisterOrganizationDelegatedAdmin(API).

Si vous avez déjà ajouté l'administrateur délégué, utilisez le compte de gestion pour créer le journal de l'organisation ou le magasin de données sur les événements dans la CloudTrail console, ou à l'aide de l' CloudTrail API AWS CLI or. Pour plus d'informations sur la création d'un journal d'organisationCréation d'un journal de suivi pour votre organisation dans la console, consultez les Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface sections, et CreateTrail(API).

Utilisation de rôles liés à un service pour AWS CloudTrail

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

Un rôle lié à un service facilite la configuration CloudTrail car vous n'avez pas à ajouter manuellement les autorisations nécessaires. CloudTrail définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul CloudTrail peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour CloudTrail

CloudTrail utilise le rôle lié au service nommé AWSServiceRoleForCloudTrail— Ce rôle lié au service est utilisé pour prendre en charge les traces de l'organisation et les banques de données sur les événements de l'organisation.

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

- `cloudtrail.amazonaws.com`

Ce rôle est utilisé pour soutenir la création et la gestion de sentiers d' CloudTrail organisation et de magasins de données sur les événements de CloudTrail Lake Organization dans CloudTrail. Pour plus d'informations, consultez Création d'un journal de suivi pour une organisation.

La CloudTrailServiceRolePolicypolitique attachée au rôle permet d' CloudTrail effectuer les actions suivantes sur les ressources spécifiées :

- Actions sur toutes les CloudTrail ressources :
  - `All`
- Actions sur toutes les AWS Organizations ressources :
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- Actions sur toutes les ressources de l'Organisation pour que le directeur de CloudTrail service répertorie les administrateurs délégués de l'organisation :
  - `organizations:ListDelegatedAdministrators`
- Actions pour désactiver la fédération Lake sur le magasin de données d'événement d'organisation :
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour CloudTrail

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un journal d'organisation ou un magasin de données sur les événements de l'organisation, que vous ajoutez un administrateur délégué dans la CloudTrail console, ou que vous utilisez l'opération AWS CLI ou API, vous CloudTrail créez le rôle lié au service pour vous s'il n'existe pas déjà.

Si vous supprimez ce rôle lié à un service et que vous devez ensuite le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un journal

d'organisation ou une banque de données sur les événements de l'organisation, ou que vous ajoutez un administrateur délégué, vous CloudTrail créez à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour CloudTrail

CloudTrail ne vous permet pas de modifier le rôle AWSServiceRoleForCloudTrail lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour CloudTrail

Il n'est pas nécessaire de supprimer le AWSServiceRoleForCloudTrail rôle manuellement. Si un Compte AWS est supprimé d'une organisation Organizations, le AWSServiceRoleForCloudTrail rôle en est automatiquement supprimé Compte AWS. Vous ne pouvez pas détacher ou supprimer des politiques du rôle lié au service AWSServiceRoleForCloudTrail dans un compte de gestion d'organisation sans supprimer le compte de l'organisation.

Vous pouvez également utiliser la console IAM AWS CLI ou l' AWS API pour supprimer manuellement le rôle lié à un service. Pour cela, vous devez commencer par nettoyer manuellement les ressources pour votre rôle lié à un service. Vous pouvez ensuite supprimer manuellement ce rôle.

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

Pour supprimer une ressource utilisée par le rôle AWSServiceRoleForCloudTrail, vous pouvez procéder de l'une des manières suivantes :

- Compte AWS Supprimez-le de l'organisation dans Organizations.
- Mettre à jour le journal de suivi afin qu'il ne soit plus le journal d'activité d'une organisation. Pour plus d'informations, consultez Mise à jour d'un journal de suivi.
- Mettre à jour le magasin de données d'événement afin qu'il ne soit plus un magasin de données d'événement d'organisation. Pour plus d'informations, consultez Mettre à jour un magasin de données d'événements avec la console.

- Supprimer le journal de suivi. Pour plus d'informations, consultez Suppression d'un journal de suivi.
- Supprimer le magasin de données d'événement. Pour plus d'informations, consultez Supprimer un magasin de données d'événements à l'aide de la console.

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

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

Régions prises en charge pour les rôles CloudTrail liés à un service

CloudTrail prend en charge l'utilisation de rôles liés aux services dans tous les domaines Régions AWS où et CloudTrail Organizations sont tous deux disponibles. Pour de plus amples informations, veuillez consulter Points de terminaison Service AWS dans le Références générales AWS.

AWS politiques gérées pour AWS CloudTrail

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser des politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

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

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité,

il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : **AWSCloudTrail_ReadOnlyAccess**

Une identité utilisateur associée à la AWSCloudTrail_ReadOnlyAccesspolitique associée à son rôle peut effectuer des actions en lecture seule CloudTrail, telles que des `Describe*` actions sur des sentiers `Get*List*`, des magasins de données d'événements CloudTrail Lake ou des requêtes Lake.

AWS politique gérée : **AWSServiceRoleForCloudTrail**

La CloudTrailServiceRolePolicypolitique permet d' AWS CloudTrail effectuer des actions sur les traces de l'organisation et sur les stockages de données d'événements de l'organisation en votre nom. La politique inclut AWS Organizations les autorisations requises pour décrire et répertorier les comptes de l'organisation et les administrateurs délégués au AWS Organizations sein d'une organisation.

Cette politique inclut également les exigences AWS Glue et les AWS Lake Formation autorisations nécessaires pour désactiver la fédération Lake dans le magasin de données d'événements d'une organisation.

Cette politique est associée au rôle AWSServiceRoleForCloudTraillié au service qui permet d' CloudTrail effectuer des actions en votre nom. Vous pouvez attacher cette politique à vos utilisateurs, groupes ou rôles.

CloudTrail mises à jour des politiques AWS gérées

Afficher les détails des mises à jour des politiques AWS gérées pour CloudTrail. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS de la CloudTrail Historique du document page.

Modification	Description	Date
`CloudTrailServiceRolePolicy` – Mise à jour d'une stratégie existante	Politique mise à jour pour autoriser les actions suivantes sur le magasin de données d'événement d'une organisat	26 novembre 2023

Modification	Description	Date
	ion lorsque la fédération est désactivée : • `glue:DeleteTable` • `lakeformation:DeregisterResource`	
`AWSCloudTrail_ReadOnlyAccess` – Mise à jour d'une politique existante	CloudTrail a changé le nom de la `AWSCloudTrailReadOnlyAccess` politique en`AWSCloudTrail_ReadOnlyAccess`. De plus, la portée des autorisations dans la politique a été réduite aux CloudTrail actions. Il n'inclut plus Amazon S3 AWS KMS, ni les autorisations AWS Lambda d'action.	6 juin 2022
CloudTrail a commencé à suivre les modifications	CloudTrail a commencé à suivre les modifications apportées AWS à ses politiques gérées.	6 juin 2022

Validation de conformité pour AWS CloudTrail

Des auditeurs tiers évaluent la sécurité et AWS CloudTrail la conformité de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

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 fournissent des étapes pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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 décrivent les directives relatives aux contrôles de sécurité dans plusieurs 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, telles que la norme PCI DSS, 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 dans AWS CloudTrail

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité 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. Si vous avez spécifiquement besoin de répliquer vos fichiers CloudTrail journaux sur de plus grandes distances géographiques, vous pouvez utiliser la réplication entre régions pour vos compartiments Amazon S3 d'essai, qui permet la copie automatique et asynchrone d'objets entre des compartiments situés dans différentes régions. AWS

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

Outre l'infrastructure AWS mondiale, CloudTrail propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Des magasins de données sur les sentiers et les événements qui enregistrent les événements dans toutes les AWS régions

Lorsque vous appliquez une piste à toutes les AWS régions, elle CloudTrail crée des pistes avec des configurations identiques dans toutes les autres Régions AWS régions de la AWS partition dans laquelle vous travaillez. Lorsque AWS vous ajoutez une nouvelle région, cette configuration de sentier est automatiquement créée dans la nouvelle région.

Lorsque vous créez un magasin de données d'événements multirégional, il CloudTrail collecte les événements qui se produisent dans l'ensemble Régions AWS de votre compte.

Gestion des versions, configuration du cycle de vie et protection contre le verrouillage des objets pour les données de CloudTrail journal

Comme il CloudTrail utilise des compartiments Amazon S3 pour stocker les fichiers journaux, vous pouvez également utiliser les fonctionnalités fournies par Amazon S3 pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour plus d'informations, consultez Resilience in Amazon S3 (Résilience dans Amazon S3).

Sécurité de l'infrastructure dans AWS CloudTrail

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

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

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

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

Les meilleures pratiques de sécurité suivantes concernent également la sécurité de l'infrastructure dans CloudTrail :

- Envisager des points de terminaison d'un VPC Amazon pour l'accès au journal de suivi.
- Prise en compte des points de terminaison d'un VPC pour l'accès au compartiment Amazon S3 Pour plus d'informations, consultez la section Contrôle de l'accès depuis les points de terminaison VPC à l'aide de politiques de compartiment.
- Identifiez et auditez tous les compartiments Amazon S3 contenant des fichiers CloudTrail journaux. Envisagez d'utiliser des balises pour identifier à la fois vos CloudTrail parcours et les compartiments Amazon S3 contenant les fichiers CloudTrail journaux. Vous pouvez ensuite utiliser

des groupes de ressources pour vos CloudTrail ressources. Pour plus d'informations, voir AWS Resource Groups.

Prévention du problème de l'adjoint confus entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS CloudTrail accordent un autre service à la ressource. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `"arn:aws:cloudtrail:*:AccountID:trail/*"`. Lorsque vous incluez un caractère générique, vous devez également utiliser l'opérateur de condition `StringLike`.

La valeur de `aws:SourceArn` doit être l'ARN du journal de suivi, de l'entrepôt de données d'événement ou du canal qui utilise la ressource.

L'exemple suivant montre comment utiliser les touches de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale CloudTrail pour éviter le problème de confusion des adjoints :Politique relative aux compartiments Amazon S3 pour les résultats des requêtes CloudTrail Lake.

Bonnes pratiques de sécurité dans AWS CloudTrail

AWS CloudTrail fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Rubriques

CloudTrail meilleures pratiques en matière de sécurité des détectives

Créer un journal de suivi

Pour un enregistrement continu des événements de votre AWS compte, vous devez créer un parcours. Bien qu'il CloudTrail fournisse 90 jours d'informations sur l'historique des événements pour la gestion des événements dans la CloudTrail console sans créer de trace, il ne s'agit pas d'un enregistrement permanent et ne fournit pas d'informations sur tous les types d'événements possibles. Pour un registre permanent, et pour un registre contenant tous les types d'événements que vous spécifiez, il convient de créer un journal d'activité, qui transmet des fichiers journaux à un compartiment Amazon S3 que vous spécifiez.

Pour faciliter la gestion de vos CloudTrail données, envisagez de créer un suivi qui enregistre tous les événements de gestion Régions AWS, puis de créer des journaux supplémentaires qui enregistrent des types d'événements spécifiques pour les ressources, tels que l'activité ou les AWS Lambda fonctions du compartiment Amazon S3.

Voici quelques-unes des étapes que vous pouvez suivre:

- Créez un journal d'activité pour votre compte AWS.
- Créez un journal d'activité pour une organisation.

Appliquez les sentiers à tous Régions AWS

Pour obtenir un enregistrement complet des événements enregistrés par une identité ou un service IAM dans votre AWS compte, chaque trace doit être configurée de manière à consigner tous les Régions AWSévénements. En enregistrant tous les événements Régions AWS, vous vous assurez que tous les événements qui se produisent sur votre AWS compte sont enregistrés, quelle que soit la AWS région où ils se sont produits. Cela inclut la journalisation des événements de service mondiaux, qui sont enregistrés AWS dans une région spécifique à ce service. Lorsque vous créez un journal qui s'applique à toutes les régions, que vous CloudTrail enregistrez les événements dans chaque région et que vous CloudTrail transmettez les fichiers journaux d'événements à un compartiment S3 que vous spécifiez. Si une Région AWS est ajoutée après la création d'un journal de suivi qui s'applique à toutes les régions, cette nouvelle région est automatiquement incluse, et les événements de cette région sont journalisés. Il s'agit de l'option par défaut lorsque vous créez un parcours dans la CloudTrail console.

Voici quelques-unes des étapes que vous pouvez suivre:

- Créez un journal d'activité pour votre compte AWS .
- Mettre à jour un journal d'activité existant afin d'enregistrer les événements du journal dans toutes les Régions AWS.
- Mettez en œuvre des contrôles de détection continus pour vous assurer que tous les sentiers créés enregistrent tous les événements en Régions AWS utilisant la règle multi-region-cloud-trailactivée. AWS Config

Activer l'intégrité des fichiers CloudTrail journaux

Les fichiers journaux validés s'avèrent utiles lors d'enquêtes judiciaires et liées à la sécurité. Par exemple, un fichier journal validé permet d'affirmer que le fichier journal en question n'a pas été modifié ou que les informations d'identification d'une identité IAM donnée ont réalisé une activité API spécifique. Le processus de validation de l'intégrité des fichiers CloudTrail journaux vous permet également de savoir si un fichier journal a été supprimé ou modifié, ou de confirmer qu'aucun fichier journal n'a été envoyé à votre compte pendant une période donnée. CloudTrail la validation de l'intégrité des fichiers journaux utilise des algorithmes conformes aux normes du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection. Pour plus d'informations, consultez Activer la validation et les fichiers de validation.

Intégrer à Amazon CloudWatch Logs

CloudWatch Les journaux vous permettent de surveiller et de recevoir des alertes pour des événements spécifiques capturés par CloudTrail. Les événements envoyés à CloudWatch Logs sont ceux configurés pour être enregistrés par votre parcours. Assurez-vous donc d'avoir configuré votre ou vos sentiers pour enregistrer les types d'événements (événements de gestion et/ou événements liés aux données) que vous souhaitez surveiller.

Par exemple, vous pouvez surveiller les principaux événements liés à la sécurité et à la gestion du réseau, tels que les échecs de AWS Management Console connexion.

Voici quelques-unes des étapes que vous pouvez suivre:

- Consultez les exemples CloudWatchd'intégrations de journaux pour CloudTrail.
- Configurez votre parcours pour envoyer des événements à CloudWatch Logs.
- Envisagez de mettre en œuvre des contrôles de détection continus pour vous assurer que tous les sentiers envoient des événements à CloudWatch Logs à des fins de surveillance en utilisant la cloud-trail-cloud-watchrègle -logs-enabled. AWS Config

Utilisez Amazon GuardDuty

Amazon GuardDuty est un service de détection des menaces qui vous aide à protéger vos comptes, vos conteneurs, vos charges de travail et les données de votre AWS environnement. En utilisant des modèles d'apprentissage automatique (ML) et des fonctionnalités de détection des anomalies et des menaces, vous surveillez GuardDuty en permanence différentes sources de journaux afin d'identifier et de hiérarchiser les risques de sécurité potentiels et les activités malveillantes dans votre environnement.

Par exemple, GuardDuty détectera une éventuelle exfiltration d'informations d'identification au cas où il détecterait des informations d'identification créées exclusivement pour une instance Amazon EC2 via un rôle de lancement d'instance mais utilisées à partir d'un autre compte interne. AWS Pour plus d'informations, consultez le guide de GuardDuty l'utilisateur Amazon.

Utilisez AWS Security Hub

Surveillez votre utilisation CloudTrail en ce qui concerne les meilleures pratiques de sécurité en utilisant AWS Security Hub. Security Hub utilise des contrôles de sécurité de détection pour évaluer les configurations des ressources et les normes de sécurité afin de vous aider à vous conformer à divers cadres de conformité. Pour plus d'informations sur l'utilisation de Security Hub pour évaluer les CloudTrail ressources, consultez la section AWS CloudTrail Contrôles du Guide de AWS Security Hub l'utilisateur.

CloudTrail meilleures pratiques de sécurité préventive

Les meilleures pratiques suivantes CloudTrail peuvent vous aider à prévenir les incidents de sécurité.

Se connecter à un compartiment Amazon S3 dédié et centralisé

CloudTrail les fichiers journaux sont un journal d'audit des actions entreprises par une identité ou un AWS service IAM. L'exhaustivité, l'intégrité et la disponibilité de ces journaux est essentielle à des fins juridiques et d'audit. En vous connectant à un compartiment Amazon S3 dédié et centralisé, il est possible d'appliquer des contrôles de sécurité stricts, l'accès, et la séparation des tâches.

Voici quelques-unes des étapes que vous pouvez suivre:

- Créez un AWS compte distinct en tant que compte d'archivage des journaux. Si vous l'utilisez AWS Organizations, inscrivez ce compte dans l'organisation et envisagez de créer un journal d'organisation pour enregistrer les données de tous les AWS comptes de votre organisation.
- Si vous n'utilisez pas Organizations mais souhaitez enregistrer les données de plusieurs AWS comptes, créez une trace pour enregistrer l'activité dans ce compte d'archive de journaux. Restreignez l'accès à ce compte uniquement aux utilisateurs administratifs de confiance qui doivent avoir accès au compte et aux données d'audit.
- Dans le cadre de la création d'un suivi, qu'il s'agisse d'un suivi organisationnel ou d'un suivi pour un seul AWS compte, créez un compartiment Amazon S3 dédié pour stocker les fichiers journaux de ce suivi.
- Si vous souhaitez enregistrer l'activité de plusieurs AWS comptes, modifiez la politique de compartiment pour autoriser la journalisation et le stockage de fichiers journaux pour tous les AWS comptes sur lesquels vous souhaitez enregistrer l'activité du AWS compte.
- Si vous n'utilisez pas de journal d'activité d'une organisation, créez des journaux d'activité dans l'ensemble de vos comptes AWS , en spécifiant le compartiment Amazon S3 dans le compte du journal d'archivage.

Utiliser le chiffrement côté serveur avec des clés gérées AWS KMS

Par défaut, les fichiers journaux fournis par votre compartiment S3 sont chiffrés CloudTrail à l'aide d'un chiffrement côté serveur avec une clé KMS (SSE-KMS). Pour utiliser SSE-KMS avec CloudTrail, vous devez créer et gérer une AWS KMS keyclé KMS.

> **Note**
>
> Si vous utilisez SSE-KMS et la validation de fichiers journaux, et que vous avez modifié votre politique de compartiment Amazon S3 de façon à autoriser uniquement les fichiers chiffrés SSE-KMS, vous ne serez pas en mesure de créer des journaux d'activité qui utilisent ce compartiment, à moins de modifier votre stratégie de compartiment pour spécifiquement autoriser le chiffrement AES256, comme illustré dans l'exemple de ligne de stratégie suivant.
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

Voici quelques-unes des étapes que vous pouvez suivre:

- Vérifier les avantages de chiffrer vos fichiers journaux avec SSE-KMS.
- Créer une clé KMS pour le chiffrement des fichiers journaux.
- Configurer le chiffrement des fichiers journaux pour vos journaux de suivi.
- Envisagez de mettre en œuvre des contrôles de détection continus pour vous assurer que toutes les pistes chiffrent les fichiers journaux avec SSE-KMS en utilisant la règle dans cloud-trail-encryption-enabled. AWS Config

Ajoutez une clé de condition à la politique de rubrique Amazon SNS par défaut

Lorsque vous configurez un suivi pour envoyer des notifications à Amazon SNS, vous ajoutez une déclaration CloudTrail de politique à votre politique d'accès aux rubriques SNS qui permet d'envoyer du contenu CloudTrail à une rubrique SNS. Pour des raisons de sécurité, nous recommandons d'ajouter une clé de condition `aws:SourceArn` (ou facultativement`aws:SourceAccount`) à la déclaration CloudTrail de politique. Cela permet d'empêcher tout accès non autorisé de compte à votre rubrique SNS. Pour en savoir plus, consultez Politique relative aux rubriques Amazon SNS pour CloudTrail.

Mettre en œuvre l'accès au moindre privilège pour les compartiments Amazon S3 de stockage des fichiers journaux

CloudTrail les trails enregistrent les événements dans un compartiment Amazon S3 que vous spécifiez. Ces fichiers journaux contiennent un journal d'audit des actions entreprises par les identités et les AWS services IAM. L'intégrité et l'exhaustivité de ces fichiers journaux sont cruciales à des fins d'audit et judiciaires. Afin de garantir cette intégrité, vous devez respecter le principe du moindre

privilège lorsque vous créez ou modifiez l'accès à un compartiment Amazon S3 utilisé pour stocker des fichiers CloudTrail journaux.

Suivez les étapes suivantes:

- Examinez la politique du compartiment Amazon S3 pour tous les compartiments où vous stockez des fichiers journaux et ajustez-le au besoin pour supprimer tout accès inutile. Cette politique de compartiment sera générée pour vous si vous créez un journal à l'aide de la CloudTrail console, mais elle peut également être créée et gérée manuellement.
- En tant que bonne pratique en matière de sécurité, veillez à ajouter manuellement une clé de condition `aws:SourceArn` de la politique de compartiment. Pour plus d'informations, consultez Politique relative aux compartiments Amazon S3 pour CloudTrail.
- Si vous utilisez le même compartiment Amazon S3 pour stocker les fichiers journaux de plusieurs AWS comptes, suivez les instructions relatives à la réception de fichiers journaux pour plusieurs comptes.
- Si vous utilisez le journal d'activité d'une organisation, assurez-vous de suivre les consignes pour les journaux d'activité de l'organisation, et d'examiner l'exemple de politique pour un compartiment Amazon S3 pour un journal d'activité d'une organisation dans Création d'un parcours pour une organisation à l'aide du AWS Command Line Interface.
- Consultez la documentation de sécurité Amazon S3 et l'exemple de démonstration relative à la sécurisation d'un compartiment.

Activer la fonction Supprimer MFA dans le compartiment Amazon S3 de stockage des fichiers journaux

La configuration de l'authentification multifactorielle (MFA) garantit que toute tentative de modifier l'état de gestion des versions de votre compartiment ou de supprimer une version d'un objet nécessite un niveau d'authentification supplémentaire. Ainsi, même si un utilisateur acquiert le mot de passe d'un utilisateur IAM disposant d'autorisations pour supprimer définitivement des objets Amazon S3, vous pouvez toujours empêcher les opérations susceptibles de compromettre vos fichiers journaux.

Voici quelques-unes des étapes que vous pouvez suivre:

- Consultez les instructions concernant Supprimer MFA dans le Guide de l'utilisateur d'Amazon Simple Storage Service.
- Ajoutez une politique de compartiment Amazon S3 pour pouvoir solliciter la MFA.

> **Note**
>
> Vous ne pouvez pas utiliser la suppression MFA avec des configurations de cycle de vie. Pour en savoir plus sur les configurations de cycle de vie et sur leur interaction avec d'autres configurations, veuillez consulter Cycle de vie et autres configurations de compartiment dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

Configurez le système de gestion du cycle de vie des objets dans le compartiment Amazon S3, qui est le lieu pour stocker des fichiers journaux

Par CloudTrail défaut, les fichiers journaux sont stockés indéfiniment dans le compartiment Amazon S3 configuré pour le suivi. Vous pouvez utiliser les règles de gestion du cycle de vie des objets Amazon S3 pour définir votre propre politique de conservation pour mieux répondre aux besoins de votre entreprise et des audits. Par exemple, vous pouvez vouloir archiver les fichiers journaux vieux de plus d'un an dans Amazon Glacier, ou supprimer des fichiers journaux après l'écoulement d'un certain délai.

> **Note**
>
> La configuration du cycle de vie des compartiments activés pour MFA (authentification multi-facteur) n'est pas prise en charge.

Limiter l'accès à la AWSCloudTrail_FullAccess politique

Les utilisateurs dotés de AWSCloudTrail_FullAccesscette politique ont la possibilité de désactiver ou de reconfigurer les fonctions d'audit les plus sensibles et les plus importantes de leurs AWS comptes. Cette politique n'est pas destinée à être partagée ou appliquée de manière générale aux identités IAM de votre AWS compte. Limitez l'application de cette politique au moins de personnes possible, celles que vous attendez d'agir en tant qu'administrateurs de AWS compte.

Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS)

Par défaut, les fichiers journaux fournis par votre compartiment sont chiffrés CloudTrail à l'aide d'un chiffrement côté serveur avec une clé KMS (SSE-KMS). Si vous n'activez pas le chiffrement SSE-KMS, vos journaux sont chiffrés à l'aide du chiffrement SSE-S3.

> **Note**
>
> L'activation du chiffrement côté serveur chiffre les fichiers journaux, mais pas les fichiers de valeur de hachage avec SSE-KMS. Les fichiers de valeur de hachage sont chiffrés avec des Amazon S3-managed encryption keys (SSE-S3) (clés de chiffrement gérées par Amazon S3 (SSE-S3)).
> Si vous utilisez un compartiment S3 existant avec une clé de compartiment S3, vous CloudTrail devez être autorisé dans la politique des clés à utiliser les AWS KMS actions `GenerateDataKey` et`DescribeKey`. Si `cloudtrail.amazonaws.com` n'est pas accordé ces autorisations dans la politique de clé, vous ne pouvez pas créer ou mettre à jour un journal de suivi.

Pour utiliser SSE-KMS avec CloudTrail, vous devez créer et gérer une clé KMS, également appelée. AWS KMS key Vous attachez une politique à la clé qui détermine quels utilisateurs peuvent utiliser la clé pour chiffrer et déchiffrer CloudTrail les fichiers journaux. Le déchiffrement est transparent via S3. Lorsque les utilisateurs autorisés de la clé lisent les fichiers CloudTrail journaux, S3 gère le déchiffrement et les utilisateurs autorisés peuvent lire les fichiers journaux sous forme non chiffrée.

Cette méthode offre les avantages suivants :

- Vous pouvez créer et gérer les clés de chiffrement KMS vous-même.
- Vous pouvez utiliser une seule clé KMS pour chiffrer et déchiffrer les fichiers journaux de plusieurs comptes dans toutes les régions.
- Vous pouvez contrôler qui peut utiliser votre clé pour chiffrer et déchiffrer CloudTrail les fichiers journaux. Vous pouvez attribuer des autorisations pour la clé aux utilisateurs de votre organisation selon vos besoins.
- Vous bénéficiez d'une sécurité renforcée. Grâce à cette fonctionnalité, la lecture des fichiers journaux, requiert les autorisations suivantes :
  - Un utilisateur doit avoir des autorisations de lecture S3 pour le compartiment qui contient les fichiers journaux.
  - Un utilisateur doit également avoir une politique ou un rôle permettant des autorisations de déchiffrement par la politique clé KMS.
- Comme S3 déchiffre automatiquement les fichiers journaux pour les demandes des utilisateurs autorisés à utiliser la clé KMS, le chiffrement SSE-KMS des fichiers CloudTrail journaux est rétrocompatible avec les applications qui lisent les données des journaux. CloudTrail

> **Note**
>
> La clé KMS que vous choisissez doit être créée dans la même AWS région que le compartiment Amazon S3 qui reçoit vos fichiers journaux. Par exemple, si les fichiers journaux vont être stockés dans un compartiment de la région USA Est (Ohio), vous devez créer ou choisir une clé KMS qui a été créée dans cette région. Pour vérifier la région pour un compartiment Amazon S3, examinez ses propriétés dans la console Amazon S3.

Activation du chiffrement de fichier journaux

> **Note**
>
> Si vous créez une clé KMS dans la CloudTrail console, CloudTrail ajoute les sections de politique de clé KMS requises pour vous. Suivez ces procédures si vous avez créé une clé dans la console IAM ou AWS CLI si vous devez ajouter manuellement les sections de stratégie requises.

Pour activer le chiffrement SSE-KMS pour les fichiers CloudTrail journaux, effectuez les étapes de haut niveau suivantes :

1. Créer une clé KMS.

   - Pour plus d'informations sur la création d'une clé KMS avec le AWS Management Console, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.
   - Pour plus d'informations sur la création d'une clé KMS avec le AWS CLI, voir create-key.

   > **Note**
   >
   > La clé KMS que vous choisissez doit être dans la même région que le compartiment S3 qui reçoit vos fichiers-journaux. Pour vérifier la région pour un compartiment S3, examinez les propriétés du compartiment dans la console S3.

2. Ajoutez des sections de politique à la clé qui permettent CloudTrail de chiffrer les fichiers journaux et aux utilisateurs de les déchiffrer.

- Pour plus d'informations sur ce qu'il convient d'inclure dans la politique, consultez la page Configurer les politiques AWS KMS clés pour CloudTrail.

> **Warning**
>
> Veillez à inclure les autorisations de déchiffrement dans les règles pour tous les utilisateurs qui ont besoin de lire les fichiers journaux. Si vous n'effectuez pas cette étape avant d'ajouter la clé à la configuration de votre journal d'activité, les utilisateurs ne disposant pas d'autorisations de déchiffrement ne peuvent pas lire les fichiers chiffrés jusqu'à ce que vous leur accordiez ces autorisations.

- Pour plus d'informations sur la modification d'une politique avec la console IAM, consultez Editing a Key Policy (Modification d'une politique de clé) dans le Guide du développeur AWS Key Management Service .
- Pour plus d'informations sur l'attachement d'une politique à une clé KMS à l'aide du AWS CLI, consultez put-key-policy.

3. Mettez à jour votre historique pour utiliser la clé KMS pour laquelle vous avez modifié la politique CloudTrail.

   - Pour mettre à jour la configuration de votre parcours à l'aide de la CloudTrail console, consultezMise à jour d'une ressource pour qu'elle utilise votre clé KMS.
   - Pour mettre à jour la configuration de votre parcours à l'aide du AWS CLI, voirActivation et désactivation du chiffrement des fichiers CloudTrail journaux à l'aide du AWS CLI.

CloudTrail prend également en charge les clés AWS KMS multirégionales. Pour plus d'informations, consultez la section Utilisation de clés multi-régions dans le Guide du développeur AWS Key Management Service .

La section suivante décrit les sections de politique avec lesquelles votre politique de clé KMS doit être utilisée CloudTrail.

Octroi d'autorisations pour la création d'une clé KMS

Vous pouvez autoriser les utilisateurs à créer une AWS KMS key avec la `AWSKeyManagementServicePowerUser` politique.

Accorder l'autorisation de créer une clé KMS.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Sélectionnez le groupe ou l'utilisateur auquel vous souhaitez accorder l'autorisation.
3. Sélectionnez Permissions (Autorisations), puis choisir Attach Policy (Attacher une politique).
4. Recherchez AWSKeyManagementServicePowerUser, choisissez la politique, puis choisissez Attach Policy (Attacher une politique).

   L'utilisateur détient maintenant l'autorisation de créer une clé KMS. Pour plus d'informations sur la création de politiques, consultez la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

Configurer les politiques AWS KMS clés pour CloudTrail

Vous pouvez créer un AWS KMS key de trois manières :

- La CloudTrail console
- La console AWS de gestion
- Le AWS CLI

> **Note**
>
> Si vous créez une clé KMS dans la CloudTrail console, CloudTrail ajoute la politique de clé KMS requise pour vous. Vous n'avez pas besoin d'ajouter manuellement les déclarations de politique. Consultez Politique de clé KMS par défaut créée dans CloudTrail la console.

Si vous créez une clé KMS dans le AWS Management ou le AWS CLI, vous devez ajouter des sections de politique à la clé afin de pouvoir l'utiliser avec CloudTrail. La politique doit autoriser CloudTrail l'utilisation de la clé pour chiffrer vos fichiers journaux et vos magasins de données d'événements, et autoriser les utilisateurs que vous spécifiez à lire les fichiers journaux sous forme non chiffrée.

Consultez les ressources suivantes :

- Pour créer une clé KMS avec le AWS CLI, voir create-key.

- Pour modifier une politique clé KMS pour CloudTrail, consultez la section Modification d'une politique clé dans le guide du AWS Key Management Service développeur.
- Pour obtenir des informations techniques sur le mode d' CloudTrail utilisation AWS KMS, reportez-vous AWS KMSà la section Mode AWS CloudTrail d'emploi du guide du AWS Key Management Service développeur.

Sections de politique clés KMS requises pour une utilisation avec CloudTrail

Si vous avez créé une clé KMS à l'aide de la console de AWS gestion ou du AWS CLI, vous devez au minimum ajouter les instructions suivantes à votre politique de clé KMS pour qu'elle fonctionne CloudTrail.

Rubriques

- Éléments de politique clé KMS requis pour les journaux de suivi
- Éléments de politique clé KMS requis pour les magasins de données d'événement

Éléments de politique clé KMS requis pour les journaux de suivi

1. Activez les autorisations de chiffrement du CloudTrail journal. veuillez consulter Attribution des autorisations de chiffrement.
2. Activez les autorisations de déchiffrement du CloudTrail journal. Consultez Attribution des autorisations de déchiffrement. Si vous utilisez un compartiment S3 existant avec une clé S3 Bucket Key (Clé de compartiment S3), les autorisations `kms:Decrypt` sont nécessaires pour créer ou mettre à jour un journal de suivi en utilisant le chiffrement SSE-KMS activé.
3. Activez CloudTrail cette option pour décrire les propriétés des clés KMS. Consultez Activer CloudTrail pour décrire les propriétés des clés KMS.

Comme bonne pratique en matière de sécurité, ajoutez une clé de condition `aws:SourceArn` à la politique de clé KMS. La clé de condition globale IAM `aws:SourceArn` permet de garantir que la clé KMS est CloudTrail utilisée uniquement pour un ou plusieurs sentiers spécifiques. La valeur de `aws:SourceArn` est toujours l'ARN du journal d'activité (ou tableau des ARN du journal d'activité) qui utilise la clé KMS. Veillez à ajouter la clé de condition `aws:SourceArn` des politiques de clé KMS pour les journaux d'activité existants.

La clé de condition `aws:SourceAccount` est également prise en charge, mais elle n'est pas recommandée. La valeur de `aws:SourceAccount` est l'ID de compte du propriétaire du journal d'activité ou, pour les journaux d'activité de l'organisation, l'ID du compte de gestion.

> **Important**
>
> Lorsque vous ajoutez les nouvelles sections à votre politique de clé KMS, ne changez pas les sections existantes dans la politique.
> Si le chiffrement est activé lors d'un suivi et que la clé KMS est désactivée, ou si la politique de clé KMS n'est pas correctement configurée CloudTrail, les journaux CloudTrail ne peuvent pas être envoyés.

Éléments de politique clé KMS requis pour les magasins de données d'événement

1. Activez les autorisations de chiffrement du CloudTrail journal. veuillez consulter Attribution des autorisations de chiffrement.
2. Activez les autorisations de déchiffrement du CloudTrail journal. veuillez consulter Attribution des autorisations de déchiffrement.
3. Accordez aux utilisateurs et aux rôles l'autorisation de chiffrer et de déchiffrer les données d'événement avec la clé KMS.

   Lorsque vous créez un magasin de données d'événement et le chiffrez avec une clé KMS, ou que vous exécutez des requêtes sur un magasin de données d'événement que vous chiffrez avec une clé KMS, vous devez avoir un accès en écriture à la clé KMS. La politique de clé KMS doit avoir accès à la banque de données d'événements CloudTrail, et la clé KMS doit être gérable par les utilisateurs qui exécutent des opérations (telles que des requêtes) sur le magasin de données d'événements.
4. Activez CloudTrail cette option pour décrire les propriétés des clés KMS. veuillez consulter Activer CloudTrail pour décrire les propriétés des clés KMS.

Les clés de condition `aws:SourceArn` et `aws:SourceAccount` ne sont pas prises en charge dans les politiques relatives aux clés KMS pour les magasins de données d'événement.

> **Important**
>
> Lorsque vous ajoutez les nouvelles sections à votre politique de clé KMS, ne changez pas les sections existantes dans la politique.
> Si le chiffrement est activé sur un magasin de données d'événements et que la clé KMS est désactivée ou supprimée, ou si la politique de clé KMS n'est pas correctement configurée CloudTrail, vous CloudTrail ne pouvez pas transmettre d'événements à votre magasin de données d'événements.

Attribution des autorisations de chiffrement

Example CloudTrail Autoriser le chiffrement des journaux pour le compte de comptes spécifiques

CloudTrail nécessite une autorisation explicite pour utiliser la clé KMS afin de chiffrer les journaux pour le compte de comptes spécifiques. Afin de spécifier un compte, ajoutez l'instruction requise suivante à votre politique de clé KMS et remplacez *`account-id`*, *`region`* et *`trailName`* par les valeurs appropriées pour votre configuration. Vous pouvez ajouter des identifiants de compte supplémentaires à la `EncryptionContext` section pour permettre à ces comptes d' CloudTrail utiliser votre clé KMS pour chiffrer les fichiers journaux.

Comme bonne pratique en matière de sécurité, ajoutez une clé de condition `aws:SourceArn` à la politique de clé KMS pour un journal de suivi. La clé de condition globale IAM `aws:SourceArn` permet de garantir que la clé KMS est CloudTrail utilisée uniquement pour un ou plusieurs sentiers spécifiques.

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
         "StringLike": {
```

```
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
          }
    }
}
```

Une politique relative à une clé KMS utilisée pour chiffrer les journaux du magasin de données d'événements de CloudTrail Lake ne peut pas utiliser les clés de condition `aws:SourceArn` ou`aws:SourceAccount`. Voici un exemple de politique de clé KMS pour un magasin de données d'événement.

```
{
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

L'exemple de déclaration de politique suivant illustre comment un autre compte peut utiliser votre clé KMS pour chiffrer CloudTrail les journaux.

Scénario

- Votre clé KMS se trouve dans le compte *111111111111*.
- Le compte *222222222222* et vous-même chiffrerez les journaux.

Dans la politique, vous ajoutez un ou plusieurs comptes chiffrés avec votre clé au CloudTrail EncryptionContext. Cela se limite CloudTrail à l'utilisation de votre clé pour chiffrer les journaux uniquement pour les comptes que vous spécifiez. Lorsque vous donnez au root du compte *222222222222* l'autorisation de chiffrer les journaux, il délègue à l'administrateur du compte l'autorisation de chiffrer les autorisations nécessaires aux autres utilisateurs de ce compte. Pour ce faire, l'administrateur du compte modifie les politiques associées à ces utilisateurs IAM.

Comme bonne pratique en matière de sécurité, ajoutez une clé de condition `aws:SourceArn` à la politique de clé KMS. La clé de condition globale IAM `aws:SourceArn` permet de garantir que la clé KMS est CloudTrail utilisée uniquement pour les sentiers spécifiés. Cette condition n'est pas prise en charge dans les stratégies de clé KMS pour les entrepôts de données d'événement.

Déclaration de politique de clé KMS :

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Pour plus d'informations sur la modification d'une politique de clé KMS à utiliser avec CloudTrail, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur.

Attribution des autorisations de déchiffrement

Avant d'ajouter votre clé KMS à votre CloudTrail configuration, il est important d'accorder des autorisations de déchiffrement à tous les utilisateurs qui en ont besoin. Les utilisateurs disposant d'autorisations de chiffrement, mais pas de déchiffrement ne peuvent pas lire les journaux chiffrés. Si vous utilisez un compartiment S3 existant avec une clé S3 Bucket Key (Clé de compartiment S3), les autorisations `kms:Decrypt` sont nécessaires pour créer ou mettre à jour un journal de suivi en utilisant le chiffrement SSE-KMS activé.

Activer les autorisations de déchiffrement du CloudTrail journal

Les utilisateurs de votre clé doivent disposer d'autorisations explicites pour lire les CloudTrail fichiers journaux chiffrés. Pour permettre aux utilisateurs de lire les journaux chiffrés, ajoutez l'instruction obligatoire suivante à votre stratégie de clé KMS, en modifiant la section `Principal` pour ajouter une ligne pour chaque principal que vous souhaitez pouvoir déchiffrer en utilisant votre clé KMS.

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Voici un exemple de politique requise pour autoriser le principal du CloudTrail service à déchiffrer les journaux de suivi.

```
{
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Une politique de déchiffrement pour une clé KMS utilisée avec un magasin de données d'événements CloudTrail Lake est similaire à la suivante. Les ARN d'utilisateur ou de rôle spécifiés comme valeurs pour `Principal` doivent déchiffrer les autorisations pour créer ou mettre à jour des magasins de données d'événement, exécuter des requêtes ou obtenir des résultats de requêtes.

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
```

```
        "Principal": {
            "AWS": "arn:aws:iam::account-id:user/username"
        },
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "*"
    }
```

Voici un exemple de politique requise pour permettre au principal du CloudTrail service de déchiffrer les journaux du magasin de données d'événements.

```
{
        "Sid": "Allow CloudTrail to decrypt an event data store",
        "Effect": "Allow",
        "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
        "Action": "kms:Decrypt",
        "Resource": "*"
}
```

Autoriser les utilisateurs de votre compte à déchiffrer les journaux de suivi avec votre clé KMS

Exemple

Cette déclaration de politique illustre la façon d'autoriser un utilisateur ou un rôle dans votre compte à utiliser votre clé pour lire les journaux chiffrés dans le compartiment S3 de votre compte.

Example Scénario

- Votre clé KMS, votre compartiment S3 et l'utilisateur IAM Bob se trouvent dans le compte *111111111111*.
- Vous autorisez Bob, utilisateur IAM, à déchiffrer CloudTrail les journaux dans le compartiment S3.

Dans la politique clé, vous activez les autorisations de déchiffrement du CloudTrail journal pour l'utilisateur IAM Bob.

Déclaration de politique de clé KMS :

```
{
```

```
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Autoriser les utilisateurs d'autres comptes à déchiffrer les journaux de suivi avec votre clé KMS

Vous pouvez autoriser les utilisateurs d'autres comptes à utiliser votre clé KMS pour déchiffrer les journaux de suivi, mais pas les journaux du magasin de données d'événement. Les modifications à apporter à votre politique de clé dépendent du fait que le compartiment S3 se trouve dans votre compte ou dans un autre compte.

Autoriser les utilisateurs d'un compartiment dans un autre compte à déchiffrer les journaux

Exemple

Cette déclaration de politique montre comment autoriser un utilisateur IAM ou un rôle dans un autre compte à utiliser votre clé pour lire des journaux chiffrés d'un compartiment S3 dans l'autre compte.

Scénario

- Votre clé KMS se trouve dans le compte *111111111111*.
- L'utilisatrice IAM Alice et le compartiment S3 sont dans le compte *222222222222*.

Dans ce cas, vous CloudTrail autorisez le déchiffrement des journaux sous compte*222222222222*, et vous autorisez la politique utilisateur IAM d'Alice à utiliser votre clé*KeyA*, qui est enregistrée dans le compte. *111111111111*

Déclaration de stratégie de clé KMS :

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Déclaration de politique utilisateur IAM d'Alice :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

Autoriser les utilisateurs d'un autre compte à déchiffrer les journaux de suivi de votre compartiment

Example

Cette politique illustre la façon dont un autre compte peut utiliser votre clé pour lire les journaux chiffrés à partir de votre compartiment S3.

Example Scénario

- Votre clé KMS et le compartiment S3 sont dans le compte *111111111111*.
- L'utilisateur qui lit les journaux dans votre compartiment est dans le compte *222222222222*.

Pour activer ce scénario, vous activez les autorisations de déchiffrement pour le rôle IAM CloudTrailReadRoledans votre compte, puis vous autorisez l'autre compte à assumer ce rôle.

Déclaration de politique de clé KMS :

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRoledéclaration de politique relative aux entités de confiance :

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

Pour plus d'informations sur la modification d'une politique de clé KMS à utiliser avec CloudTrail, consultez la section Modification d'une politique clé dans le guide du AWS Key Management Service développeur.

Activer CloudTrail pour décrire les propriétés des clés KMS

CloudTrail nécessite la capacité de décrire les propriétés de la clé KMS. Pour activer cette fonctionnalité, ajoutez l'instruction obligatoire suivante telle quelle à votre politique de clé KMS. Cette déclaration n'accorde CloudTrail aucune autorisation au-delà des autres autorisations que vous spécifiez.

Comme bonne pratique en matière de sécurité, ajoutez une clé de condition `aws:SourceArn` à la politique de clé KMS. La clé de condition globale IAM `aws:SourceArn` permet de garantir que la clé KMS est CloudTrail utilisée uniquement pour un ou plusieurs sentiers spécifiques.

```
{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Pour plus d'informations sur la modification des politiques de clé KMS, consultez Modification d'une politique de clé dans le Guide du développeur AWS Key Management Service .

Politique de clé KMS par défaut créée dans CloudTrail la console

Si vous créez un AWS KMS key dans la CloudTrail console, les politiques suivantes sont automatiquement créées pour vous. La politique permet les autorisations suivantes :

- Autorise les autorisations Compte AWS (root) pour la clé KMS.
- Permet CloudTrail de chiffrer les fichiers journaux sous la clé KMS et de décrire la clé KMS.
- Autorise tous les utilisateurs dans les comptes spécifiés à déchiffrer les fichiers journaux.
- Autorise tous les utilisateurs dans le compte spécifié à créer un alias KMS pour la clé KMS.
- Active le déchiffrement de journaux entre comptes pour l'ID de compte du compte qui a créé le journal d'activité.

Rubriques

Politique de clé KMS par défaut pour les magasins de données d'événements CloudTrail Lake

Voici la politique par défaut créée pour un AWS KMS key que vous utilisez avec un magasin de données d'événements dans CloudTrail Lake.

```
{
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores. Created
 ${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
```

```
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

Politique de clé KMS par défaut pour les journaux de suivi

Voici la politique par défaut créée pour un AWS KMS key que vous utilisez avec un trail.

> **Note**
>
> La politique comprend une instruction permettant aux comptes croisés de déchiffrer les fichiers journaux avec la clé KMS.

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:root",
                    "arn:aws:iam::account-id:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        }
    ]
}
```

Mise à jour d'une ressource pour qu'elle utilise votre clé KMS

Dans la AWS CloudTrail console, mettez à jour un journal ou un magasin de données d'événements pour utiliser une AWS Key Management Service clé. Sachez que l'utilisation de votre propre clé KMS entraîne des AWS KMS coûts de chiffrement et de déchiffrement. Pour plus d'informations, consultez Tarification d'AWS Key Management Service.

Rubriques

- Mettre à jour un journal de suivi pour utiliser une clé KMS
- Mettre à jour un magasin de données d'événement pour qu'il utilise une clé KMS

Mettre à jour un journal de suivi pour utiliser une clé KMS

Pour mettre à jour un journal afin d'utiliser AWS KMS key celui pour lequel vous l'avez modifié CloudTrail, procédez comme suit dans la CloudTrail console.

> **Note**
>
> Le fait de mettre à jour un journal de suivi selon la procédure suivante chiffre les fichiers journaux, mais pas les fichiers de valeur de hachage avec des SSE-KMS. Les fichiers de valeur de hachage sont chiffrés avec des Amazon S3-managed encryption keys (SSE-S3) (clés de chiffrement gérées par Amazon S3 (SSE-S3)).
> Si vous utilisez un compartiment S3 existant avec une clé de compartiment S3, vous CloudTrail devez être autorisé dans la politique des clés à utiliser les AWS KMS actions `GenerateDataKey` et`DescribeKey`. Si `cloudtrail.amazonaws.com` n'est pas accordé ces autorisations dans la politique de clé, vous ne pouvez pas créer ou mettre à jour un journal de suivi.

Pour mettre à jour un parcours à l'aide du AWS CLI, voirActivation et désactivation du chiffrement des fichiers CloudTrail journaux à l'aide du AWS CLI.

Mettre à jour un journal de suivi de sorte qu'il utilise votre clé KMS

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Sélectionnez Trails (Journaux de suivi), puis choisissez un nom de journal de suivi.
3. Dans General details (Détails généraux), choisissez Edit (Modifier).
4. Sous Log file SSE-KMS encryption (Chiffrement SSE-KMS du fichier journal), choisissez Enabled (Activé) si vous souhaitez chiffrer vos fichiers journaux avec SSE-KMS plutôt qu'avec SSE-S3. La valeur par défaut est Activé. Si vous n'activez pas le chiffrement SSE-KMS, vos journaux sont chiffrés à l'aide du chiffrement SSE-S3. Pour plus d'informations sur le chiffrement SSE-KMS, voir Utilisation du chiffrement côté serveur avec AWS Key Management Service

(SSE-KMS). Pour plus d'informations sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3).

Choisissez Existing (Existant) pour mettre à jour votre journal de suivi avec votre AWS KMS key. Choisissez une clé KMS située dans la même région que le compartiment S3 qui reçoit vos fichiers journaux. Pour vérifier la région pour un compartiment S3, consultez ses propriétés dans la console S3.

> **Note**
>
> Vous pouvez également saisir l'ARN d'une clé à partir d'un autre compte. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS. La politique de clé doit CloudTrail autoriser l'utilisation de la clé pour chiffrer vos fichiers journaux et permettre aux utilisateurs que vous spécifiez de lire les fichiers journaux sous forme non chiffrée. Pour en savoir plus sur la modification manuelle de la politique de clés, consultez Configurer les politiques AWS KMS clés pour CloudTrail.

Dans AWS KMS Alias, spécifiez l'alias pour lequel vous avez modifié la politique à utiliser CloudTrail, dans le format `alias/ MyAliasName`. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS.

Vous pouvez saisir le nom de l'alias, son ARN ou l'ID de clé globalement unique. Si la clé KMS appartient à un autre compte, vérifiez que la politique de clé dispose des autorisations qui vous permettent de l'utiliser. La valeur peut avoir l'un des formats suivants :

- Nom d'alias : `alias/MyAliasName`
- ARN d'alias : `arn:aws:kms:region:123456789012:alias/MyAliasName`
- ARN de clé : `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de clé globalement unique : `12345678-1234-1234-1234-123456789012`

5. Choisissez Update trail (Mettre à jour un journal de suivi).

> **Note**
>
> Si la clé KMS que vous avez sélectionnée est désactivée ou est en attente de suppression, vous ne pouvez pas enregistrer le journal de suivi avec cette clé KMS.

Vous pouvez activer la clé KMS ou en choisir une autre. Pour plus d'informations, consultez État de la clé : effet sur votre clé KMS dans le Guide du développeur AWS Key Management Service .

Mettre à jour un magasin de données d'événement pour qu'il utilise une clé KMS

Pour mettre à jour un magasin de données d'événements afin d'utiliser AWS KMS key celui pour lequel vous avez modifié CloudTrail, procédez comme suit dans la CloudTrail console.

Pour mettre à jour un magasin de données d'événements à l'aide du AWS CLI, voirMettez à jour un magasin de données d'événements avec AWS CLI.

Important

La désactivation ou la suppression de la clé KMS, ou la suppression des CloudTrail autorisations associées à la clé, CloudTrail empêche l'ingestion d'événements dans le magasin de données d'événements et empêche les utilisateurs d'interroger les données du magasin de données d'événements chiffré avec la clé. Une fois que vous avez associé un magasin de données d'événement à une clé KMS, celle-ci ne peut être ni supprimée ni modifiée. Avant de désactiver ou de supprimer une clé KMS que vous utilisez avec un magasin de données d'événement, supprimez ou sauvegardez votre magasin de données d'événement.

Mettre à jour un magasin de données d'événement pour utiliser votre clé KMS

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation de gauche, choisissez Event data stores (Magasin de données d'événement) dans Lake (Lac). Choisissez un magasin de données d'événement à mettre à jour.
3. Dans General details (Détails généraux), choisissez Edit (Modifier).
4. Pour Chiffrement, si ce n'est pas déjà activé, sélectionnez Utiliser ma propre AWS KMS key pour chiffrer vos fichiers journaux avec votre propre clé KMS.

   Choisissez Existing (Existant) pour mettre à jour votre magasin de données d'événement avec votre clé KMS. Choisissez une clé KMS située dans la même région que l'entrepôt de données d'événement. Une clé provenant d'un autre compte n'est pas prise en charge.

Dans Enter AWS KMS Alias, spécifiez l'alias pour lequel vous avez modifié la politique à utiliser CloudTrail, dans le format `alias/ MyAliasName`. Pour plus d'informations, consultez Mise à jour d'une ressource pour qu'elle utilise votre clé KMS.

Vous pouvez choisir un alias ou utiliser l'identifiant de clé unique au monde. La valeur peut avoir l'un des formats suivants :

- Nom d'alias : `alias/MyAliasName`
- ARN d'alias : `arn:aws:kms:region:123456789012:alias/MyAliasName`
- ARN de clé : `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de clé globalement unique : `12345678-1234-1234-1234-123456789012`

5. Sélectionnez Enregistrer les modifications.

> **Note**
>
> Si la clé KMS que vous avez choisie est désactivée ou en attente de suppression, vous ne pouvez pas sauvegarder la configuration du magasin de données d'événement avec cette clé KMS. Vous pouvez activer la clé KMS ou en choisir une autre. Pour plus d'informations, consultez État de la clé : effet sur votre clé KMS dans le Guide du développeur AWS Key Management Service .

Activation et désactivation du chiffrement des fichiers CloudTrail journaux à l'aide du AWS CLI

Cette rubrique décrit comment activer et désactiver le chiffrement des fichiers journaux SSE-KMS à l'aide CloudTrail du. AWS CLI Pour plus d'informations, consultez la page Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS).

Rubriques

Activation du chiffrement des fichiers CloudTrail journaux à l'aide du AWS CLI

Activer le chiffrement des fichiers journaux pour un journal de suivi

1. Créez une clé avec la AWS CLI. La clé que vous créez doit se trouver dans la même région que le compartiment S3 qui reçoit vos fichiers CloudTrail journaux. Pour cette étape, vous devez utiliser la AWS KMS create-keycommande.
2. Obtenez la politique clé existante afin de pouvoir la modifier pour l'utiliser avec CloudTrail. Vous pouvez récupérer la politique clé à l'aide de la AWS KMS get-key-policycommande.
3. Ajoutez les sections requises à la politique clé afin que les utilisateurs CloudTrail puissent chiffrer et déchiffrer vos fichiers journaux. Veillez à ce que tous les utilisateurs qui lisent les fichiers journaux se voient accorder des autorisations de déchiffrage. Ne modifiez pas les sections existantes de la politique. Pour en savoir plus sur les sections de la politique à inclure, consultez Configurer les politiques AWS KMS clés pour CloudTrail.
4. Joignez le fichier de politique JSON modifié à la clé à l'aide de la AWS KMS put-key-policycommande.
5. Exécutez la `update-trail` commande CloudTrail `create-trail` ou avec le `--kms-key-id` paramètre. Cette commande activera le chiffrement des journaux.

   ```
   aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
   ```

   Le `--kms-key-id` paramètre indique la clé pour laquelle vous avez modifié la politique CloudTrail. Il peut avoir l'un des formats suivants :

   - Nom d'alias. Exemple : `alias/MyAliasName`
   - ARN d'alias. Exemple : `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
   - ARN de clé. Exemple : `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
   - ID de clé globalement unique. Exemple : `12345678-1234-1234-1234-123456789012`

   Voici un exemple de réponse :

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "my-bucket-name"
}
```

La présence de l'élément `KmsKeyId` indique que le chiffrement de fichiers journaux a été activé. Les fichiers journaux chiffrés devraient apparaître dans votre compartiment dans environ 5 minutes.

Activer le chiffrement des fichiers journaux pour un magasin de données d'événement

1. Créez une clé avec la AWS CLI. La clé que vous créez doit se trouver dans la même région que l'entrepôt de données d'événement. Pour cette étape, exécutez la AWS KMS create-keycommande.
2. Obtenez la politique clé existante à modifier pour l'utiliser avec CloudTrail. Vous pouvez obtenir la politique clé en exécutant la AWS KMS get-key-policycommande.
3. Ajoutez les sections requises à la politique clé afin que les utilisateurs CloudTrail puissent chiffrer et déchiffrer vos fichiers journaux. Veillez à ce que tous les utilisateurs qui lisent les fichiers journaux se voient accorder des autorisations de déchiffrage. Ne modifiez pas les sections existantes de la politique. Pour en savoir plus sur les sections de la politique à inclure, consultez Configurer les politiques AWS KMS clés pour CloudTrail.
4. Joignez le fichier de politique JSON modifié à la clé en exécutant la AWS KMS put-key-policycommande.
5. Exécutez la `update-event-data-store` commande CloudTrail `create-event-data-store` ou, puis ajoutez le `--kms-key-id` paramètre. Cette commande activera le chiffrement des journaux.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

Le `--kms-key-id` paramètre indique la clé pour laquelle vous avez modifié la politique CloudTrail. Il peut avoir l'un des quatre formats suivants :

- Nom d'alias. Exemple : `alias/MyAliasName`
- ARN d'alias. Exemple : `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- ARN de clé. Exemple : `arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de clé globalement unique. Exemple : `12345678-1234-1234-1234-123456789012`

Voici un exemple de réponse :

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

La présence de l'élément `KmsKeyId` indique que le chiffrement de fichiers journaux a été activé. Les fichiers journaux chiffrés devraient apparaître dans votre entrepôt de données d'événement dans environ 5 minutes.

Désactivation du chiffrement des fichiers CloudTrail journaux à l'aide du AWS CLI

Pour arrêter le chiffrement des journaux de suivi, exécutez `update-trail` et transmettez une chaîne vide au paramètre `kms-key-id` :

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

Voici un exemple de réponse :

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

L'absence de la valeur `KmsKeyId` indique que le chiffrement des fichiers journaux n'est plus activé.

> **Important**
>
> Vous ne pouvez pas arrêter le chiffrement des fichiers journaux dans un magasin de données d'événement.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation de AWS CloudTrail. Pour receConsultez les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

- Version de l'API : 01/11/2013
- Dernière mise à jour de la documentation : 2024-05-30

Modification	Description	Date
Documentation mise à jour	Ajout d'une section pour décrire comment filtrer les événements de données à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, voir Filtrer les événements de données à l'aide de sélecteurs d'événements avancés.	29 mai 2024
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données sur les flux Amazon Kinesis Data Streams et les clients de streaming à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	21 mai 2024
Documentation mise à jour	Mise à jour de la page Régions prises en charge par CloudTrail Lake pour ajouter la région Asie-Paci	16 mai 2024

	fique (Hyderabad) (ap-south -2), la région Europe (Zurich) (eu-central-2) et la région Israël (Tel Aviv) (il-central-1).	
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de CloudTrail données sur les machines à AWS Step Functions états à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	16 mai 2024
Documentation mise à jour	Ajout d'une section sur CloudTrail le coût de visualisation et l'utilisation AWS Cost Explorer. Pour plus d'informations, consultez la section Afficher vos CloudTrail coûts et votre utilisation avec AWS Cost Explorer.	14 mai 2024
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements liés aux données sur Amazon Q Apps à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	1er mai 2024

Documentation mise à jour	Améliorations organisationnelles générales apportées aux sections et aux titres de page du guide de l'utilisateur, notamment les suivantes : modification du titre de la page de référence des événements du CloudTrail journal en « Comprendre les CloudTrail événements » et ajout de descriptions des événements de gestion, des événements de données et des événements Insights. Le titre de la page des paramètres a été modifié en « Configurer CloudTrail les paramètres ». Les pages Logging data events, Logging management events et Logging Insights ont été déplacées vers la section Comprendre les CloudTrail événements. La page d'exemples de fichiers CloudTrail journaux a été déplacée vers la section des fichiers CloudTrail journaux. Ajout de pages distinctes pour répertorier les AWS CLI commandes pour les magasins de données d'événements, les requêtes et les intégrations de CloudTrail Lake.	10 avril 2024

Documentation mise à jour	Mise à jour de la page Régions prises en charge par les CloudTrail lacs pour ajouter la région Europe (Espagne) (eu-south-2).	10 avril 2024
Prise en charge de services supplémentaires	Cette version prend en charge AWS Control Catalog. Pour plus d'informations, consultez les Service AWS rubriques CloudTrail et les appels d'API Logging AWS Control Catalog à l'aide de AWS CloudTrail.	8 avril 2024
Prise en charge de services supplémentaires	Cette version est compatibl e avec AWS Deadline Cloud. Pour plus d'informations, consultez les Service AWS rubriques relatives à CloudTrai l.	2 avril 2024
Fonctionnalité ajoutée	La version de l' AWS CloudTrail événement est désormais 1.10. Pour plus d'informations, consultez la section Contenu des CloudTrai l enregistrements.	26 mars 2024
Prise en charge de services supplémentaires	Cette version prend en charge AWS Billing Conductor. Pour plus d'informations, consultez les Service AWS rubriques CloudTrail et Journalisation des appels AWS Billing Conductor d'API à l'aide de AWS CloudTrail.	12 mars 2024

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements de données sur les AWS X-Ray traces et les nœuds AWS Systems Manager gérés à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	7 mars 2024
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements de données sur les domaines Amazon Simple Workflow Service (Amazon SWF) à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	14 février 2024
Fonctionnalité ajoutée	CloudTrail a ajouté l'`ListInsightsMetricData` API. L'`ListInsightsMetricData` API renvoie les données des métriques Insights pour les pistes qui ont activé Insights. Pour plus d'informations, consultez ListInsightsMetricDatala référence de AWS CloudTrail l'API.	6 février 2024

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail des événements de données pour AWS IoT AWS IoT SiteWise, et AWS AppConfig en utilisant des sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	4 janvier 2024
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements liés aux données à AWS IoT Greengrass l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	22 décembre 2023
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région du Canada-Ouest (Calgary). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	20 décembre 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements de données pour Amazon Keyspaces (pour Apache Cassandra), AWS IoT TwinMaker Amazon RDS et en AWS Supply Chain utilisant des sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Événements liés aux données.	20 décembre 2023

Politique AWS gérée mise à jour	Mise à jour de la politique gérée CloudTrailServiceRolePolicy pour autoriser les actions suivantes sur le magasin de données d'événement d'organisation lorsque la fédération est désactivée : `glue:DeleteTable` et `lakeformation:DeregisterResource` .	26 novembre 2023
Fonctionnalité ajoutée	Vous pouvez désormais fédérer un magasin de données d'événements CloudTrail Lake pour voir les métadonnées associées au magasin de données d'événements dans le catalogue de données et exécuter AWS Glue des requêtes SQL sur les données d'événements à l'aide d'Amazon Athena. Les métadonnées des tables stockées dans le catalogue de AWS Glue données permettent au moteur de requête Athena de savoir comment rechercher, lire et traiter les données que vous souhaitez interroger. Pour plus d'informations, consultez Fédérer un magasin de données d'événement.	26 novembre 2023

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements liés aux données à AWS Cloud Map l'aide de sélecteurs d'événements avancés. Pour plus d’informations, veuillez consulter Journalisation des événements de données.	16 novembre 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données dans les messages Amazon SQS à l'aide de sélecteurs d'événements avancés. Pour plus d’informations, veuillez consulter Journalisation des événements de données.	16 novembre 2023

Fonctionnalité ajoutée	CloudTrail Lake propose désormais deux options de tarification pour les magasins de données événement ielles : une tarification de rétention extensible sur un an et une tarification de rétention sur sept ans. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservat ion par défaut et maximale pour le magasin de données d'événement. Avant cette version, tous les magasins de données d'événement utilisaient l'option de tarificat ion de rétention sur sept ans. Vous pouvez faire passer un magasin de données d'événements de l'option de tarification de rétention sur sept ans à l'utilisation de la tarification de rétention extensible d'un an en utilisant la CloudTrail console ou l'opération AWS CLIAPI. UpdateEventDataStore Pour plus d'informations sur les options de tarification, consultez les sections Tarificat ion AWS CloudTrail Options de tarification du magasin de données d'événement.	15 novembre 2023

Fonctionnalité ajoutée	Vous pouvez désormais collecter des événement s Insights dans CloudTrail Lake. AWS CloudTrail Insights aide AWS les utilisateurs à identifier les activités inhabitue lles associées aux appels d'API et aux taux d'erreur des API et à y répondre en analysant en permanence les événements CloudTrai l de gestion. Pour collecter des événements Insights dans CloudTrail Lake, vous avez besoin d'un magasin de données d'événements source qui enregistre les événements de gestion et active Insights et d'un magasin de données d'événements de destination qui collecte les événements Insights en fonction d'une activité d'événements de gestion inhabituelle dans le magasin de données d'événements source. Pour plus d'informa tions, voir Créer un magasin de données d'événeme nts pour les événements CloudTrail Insights et Logging Insights.	9 novembre 2023

Prise en charge de services supplémentaires	Cette version prend en charge AWS Launch Wizard. Pour plus d'informations, consultez les Service AWS rubriques CloudTrail et Journalisation des appels AWS Launch Wizard d'API à l'aide de AWS CloudTrail.	8 novembre 2023
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Bedrock. Pour plus d'informations, consultez les Service AWS rubriques relatives aux appels d'API Amazon Bedrock CloudTrail et enregistrez-les à l'aide AWS CloudTrail de.	23 octobre 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données dans les CodeWhisperer personnalisations d'Amazon à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	18 octobre 2023

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de CloudTrail données sur les bases de données et les tables Amazon Timestrea m à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	28 septembre 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données sur les rubriques Amazon SNS et les points de terminais on de la plateforme à l'aide de sélecteurs d'événements avancés. Pour plus d'informa tions, veuillez consulter Journalisation des événement s de données.	28 septembre 2023
Documentation mise à jour	Tableau ajouté pour afficher les tâches que le compte de gestion, les comptes d'administrateur délégué et les comptes de membres d'une AWS Organizations organisat ion peuvent effectuer dans le cadre de cette dernière CloudTrail. Pour plus d'informa tions, consultez Administrateur délégué de l'organisation.	25 septembre 2023

Prise en charge de services supplémentaires	Cette version prend en charge AWS Marketplace les accords. Pour plus d'informations, consultez les Service AWS rubriques CloudTrail et les accords de journalisation des appels d'API à l'aide de AWS CloudTrail.	1er septembre 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de CloudTrail données sur les flux vidéo Amazon Kinesis et les SageMaker points de terminaison Amazon à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	31 août 2023
Prise en charge de services supplémentaires	Cette version prend en charge le service de transformation des AWS applications. AWS Le service de transformation des applications est un service principal utilisé par des services tels que AWS Microservice Extractor pour .NET. Pour plus d'informations, consultez la section Services et intégrations CloudTrail pris en charge.	26 août 2023

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements de données sur AWS Private CA Connector for Active Directory à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	24 août 2023
Documentation mise à jour	Ajout de nouveaux scénarios CloudTrail Lake pour montrer comment créer des magasins de données d'événements, afficher des tableaux de bord CloudTrail Lake, copier des événements de suivi dans un magasin de données d'événements, afficher et exécuter des exemples de requêtes, et enregistrer les résultats des requêtes dans un compartiment Amazon S3 à l'aide du AWS Management Console. Pour plus d'informations, voir Scénarios pour CloudTrail Lake	16 août 2023
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région d'Israël (Tel Aviv). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	1er août 2023

Prise en charge de services supplémentaires	Cette version prend en charge AWS HealthImaging. Pour plus d'informations, consultez les sections Services et intégrations CloudTrail pris en charge et Journalisation des appels d' AWS HealthImaging API à l'aide AWS CloudTrail de.	26 juillet 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de CloudTrail données dans les magasins de AWS HealthImaging données à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	26 juillet 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données sur les canaux AWS Systems Manager de contrôle et les réseaux Amazon Managed Blockchain à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	21 juin 2023

Fonctionnalité ajoutée	Vous pouvez désormais vérifier les résultats de votre requête enregistrée dans CloudTrail Lake à l'aide de la aws cloudtrail verify-query-results commande. Pour plus d'informations, veuillez consulter Valider les résultats enregistrés d'une requête à l'aide de l' AWS CLI.	21 juin 2023
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Verified Permissions. Pour plus d'informations, consultez les services et intégrations CloudTrail pris en charge et la journalisation des appels d'API Amazon Verified Permissions à l'aide AWS CloudTrail de.	13 juin 2023
Fonctionnalité ajoutée	Vous pouvez désormais utiliser les tableaux de bord CloudTrail Lake pour visualiser les événements dans un magasin de données d'événements. Pour de plus amples informations, veuillez consulter Afficher les tableaux de bord Lake.	13 juin 2023

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données dans les magasins de politiques d'autorisation vérifiés par Amazon à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	13 juin 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements liés aux données sur un CodeWhisperer profil Amazon à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	6 juin 2023

Fonctionnalité ajoutée	Vous pouvez désormais démarrer et arrêter l'ingesti on d'événements dans les magasins de données d' CloudTrail événements. Pour plus d'informations sur l'arrêt de l'ingestion d'événements à l'aide de la console, veuillez consulter Arrêter l'ingestion d'événements par un entrepôt de données d'événement. Pour plus d'informations sur l'arrêt de l'ingestion d'événeme nts à l'aide du AWS CLI, voir Arrêter l'ingestion dans une banque de données d'événements.	2 juin 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données dans un espace de travail de journalisation à écriture anticipée Amazon EMR à l'aide de sélecteurs d'événeme nts avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	31 mai 2023

Prise en charge de services supplémentaires	Cette version prend en charge Amazon Security Lake. Pour plus d'informations, consultez les services et intégrations CloudTrail pris en charge et la journalisation des appels d'API Amazon Security Lake à l'aide AWS CloudTrail de.	30 mai 2023
Documentation mise à jour	La rubrique relative à CloudTrail l'élément UserIdentity a été mise à jour afin d'inclure un exemple et des descriptions de champs pour une demande effectuée au nom d'un utilisateur d'IAM Identity Center. Pour de plus amples informations, veuillez consulter Élément CloudTrail userIdentity.	23 mai 2023
Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque de CloudTrail traitement : aws-cloudtrail-processing-library -1.6.1.jar. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et de la bibliothèque CloudTrail de traitement sur GitHub.	23 mai 2023

Fonctionnalité ajoutée	CloudTrail Lake prend désormais en charge toutes les fonctions et tous les opérateurs Presto. Pour plus d'informations, consultez la section Contraintes SQL de CloudTrail Lake.	9 mai 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements liés aux données sur un GuardDuty détecteur Amazon à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, consultez Journalisation des événements liés aux données et Journalisation des appels GuardDuty d'API Amazon avec AWS CloudTrail.	30 mars 2023
Documentation mise à jour	Ajout d'une nouvelle section sur la création de balises de répartition des coûts définies par l'utilisateur pour les entrepôts de données d'événement. Pour plus d'informations, voir Création de balises de répartition des coûts définies par l'utilisateur pour les magasins de données d'événements CloudTrail Lake.	24 mars 2023

Prise en charge de services supplémentaires	Cette version prend en charge AWS Telco Network Builder (AWS TNB). Pour plus d'informations, consultez les services et intégrations CloudTrail pris en charge et la journalisation des appels d'API AWS Telco Network Builder à l'aide de. AWS CloudTrail	21 février 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de CloudTrail données sur les pools d'identités Amazon Cognito à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	15 février 2023
Documentation mise à jour	Ajout d'une nouvelle section sur les ressources d'apprent issage disponibles pour CloudTrail Lake. Pour plus d'informations, veuillez consulter la section Ressource s d'apprentissage (français non garanti).	9 février 2023

Fonctionnalité ajoutée	Vous pouvez désormais créer des intégrations CloudTrai l Lake avec des sources d'événements extérieures à. AWS Vous pouvez journalis er et stocker les données d'activité des utilisateurs provenant des sources que vous souhaitez dans vos environnements hybrides, telles que des applications internes ou SaaS hébergées sur site ou dans le cloud, des machines virtuelles ou des conteneurs. Pour plus d'informations, veuillez consulter la section Création d'une intégration avec une source d'événements externe à AWS (français non garanti).	31 janvier 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements de données relatifs à CloudTrail `PutAuditEvents` l'activit é sur un canal CloudTrail du lac à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	31 janvier 2023

Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région Asie-Pacifique (Melbourne). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	24 janvier 2023
Documentation mise à jour	Ajout d'une nouvelle section sur la gestion de la cohérence des données dans CloudTrai l, voir Gestion de la cohérence des données dans CloudTrail.	18 janvier 2023
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données dans les magasins de SageMaker fonctionnalités Amazon à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	27 décembre 2022
Prise en charge de services supplémentaires	Cette version prend en charge AWS Marketplace Discovery . Consultez Intégrations et services pris en charge par AWS CloudTrail.	15 décembre 2022

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail les événements liés aux données sur les composant s SageMaker des essais d'Amazon Metrics en utilisant des sélecteurs d'événements avancés. Pour plus d'informa tions, veuillez consulter Journalisation des événement s de données.	15 décembre 2022
Fonctionnalité ajoutée	Vous pouvez désormais créer un magasin de données d'événements pour inclure des éléments AWS Config de configuration, et utiliser le magasin de données d'événements pour étudier les modifications non conformes apportées à vos environne ments de production. Pour plus d'informations, voir Création d'un magasin de données d'événements pour les éléments AWS Config de configuration.	28 novembre 2022
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région Asie-Pacifique (Hyderabad). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	22 novembre 2022

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements liés aux CloudTrail données Amazon FinSpace dans les environnements à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	18 novembre 2022
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région Europe (Espagne). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	16 novembre 2022
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région Europe (Zurich). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	9 novembre 2022
Fonctionnalité ajoutée	Le compte de gestion d'une AWS Organizations organisation peut désormais ajouter un administrateur délégué chargé de gérer les CloudTrail traces et les magasins de données sur les événements de l'organisation. Pour plus d'informations, consultez Organization delegated administrator (Administrateur délégué de l'organisation).	7 novembre 2022

Fonctionnalité ajoutée	Vous pouvez désormais activer AWS Key Management Service le chiffrement pour un magasin de données d'événements CloudTrail Lake. Pour plus d'informations, consultez Créer un magasin de données d'événement.	7 novembre 2022
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les résultats d'une requête CloudTrail Lake dans un compartiment Amazon S3 lorsque vous exécutez une requête. Pour plus d'informations sur l'exécution d'une requête, consultez Exécuter une requête. Pour plus d'informations sur le téléchargement des résultats d'une requête, consultez Obtention et téléchargement des résultats enregistrés d'une requête (Français non garanti).	21 octobre 2022
Fonctionnalité ajoutée	Vous pouvez désormais copier les événements de CloudTrail randonnée dans un magasin de données d'événements CloudTrail Lake. Pour plus d'informations, voir Copier les événements du sentier vers CloudTrail Lake.	19 septembre 2022

Documentation mise à jour	Ajout de la liste des CloudWatch métriques Amazon prises en charge pour CloudTrail Lake. Pour plus d'informations, consultez la section CloudWatch Mesures prises en charge.	16 septembre 2022
Fonctionnalité ajoutée	Vous pouvez désormais consulter les chaînes CloudTrail liées au service à l'aide du. AWS CLI Pour plus d'informations, consultez la section Affichage des chaînes liées à un service à l' CloudTrail aide du. AWS CLI	9 septembre 2022
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région du Moyen-Orient (EAU). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	30 août 2022

Fonctionnalité modifiée	CloudTrail a changé le nom de la politique gérée `AWSCloudTrailReadOnlyAccess` en`AWSCloudTrail_ReadOnlyAccess` . Les autorisations de cette politique ont été réduites. Par défaut, la politique n'autorise plus à répertorier tous les compartiments, AWS Lambda fonctions ou AWS KMS alias Amazon S3. Pour plus d'informations, veuillez consulter Accès en lecture seule.	6 juin 2022
Fonctionnalité modifiée	En tant que bonne pratique en matière de sécurité, vous pouvez désormais ajouter une clé de condition `aws:SourceArn` ou `aws:SourceAccount` pour un bloc de vérification ACL `s3:GetBucketAcl` dans une politique de compartiment Amazon S3. Pour plus d'informations, consultez Configurer les politiques de compartiment Amazon S3 pour CloudTrail.	11 mai 2022

Fonctionnalité modifiée	À partir du 24 février 2022, j' AWS CloudTrail ai commencé à modifier les valeurs des `sourceIPAddress` champs `userAgent` et dans tous les cas liés à une AWS Management Console session au cours de laquelle un client proxy était utilisé. Pour ces événements, CloudTrail remplace les valeurs des `sourceIPAddress` champs `userAgent` et par`AWS Internal`. CloudTraila apporté cette modification pour normaliser la façon dont il enregistre les informati ons relatives aux actions de service dans tous les AWS services. Pour plus d'informa tions, consultez la section Contenu des CloudTrail enregistrements.	12 avril 2022
Prise en charge de services supplémentaires	Cette version est compatibl e avec Amazon GameSpark s. Consultez Intégrations et services pris en charge par AWS CloudTrail.	24 mars 2022
Prise en charge de services supplémentaires	Cette version prend en charge le service de gestion AWS App Mesh Envoy. Consultez Intégrations et services pris en charge par AWS CloudTrail.	18 mars 2022

Documentation mise à jour	De nouveaux exemples de requêtes ont été ajoutés pour CloudTrail Lake, une nouvelle fonctionnalité qui vous permet d'exécuter des requêtes SQL précises à champs multiples sur vos événements. De plus, un nouveau champ, `BytesScanned` , a été ajouté aux résultats des métadonnées de requête des opérations `DescribeQuery` et `GetQueryResults` . Pour plus d'informations, consultez la section Travailler avec CloudTrail Lake.	4 mars 2022

Fonctionnalité modifiée	CloudTrail supprime désormais l'ID de compte du propriétaire du compartiment Amazon S3 dans le `resources` bloc d'un événement de données si les deux conditions suivantes sont remplies : l'appel d'API de l'événement de données provient d'un AWS compte différent de celui du propriétaire du compartiment Amazon S3, et l'appelant de l'API a reçu une `AccessDenied` erreur qui ne concernait que le compte de l'appelant. Pour plus d'information, consultez traitement des ID de compte de propriétaire du compartiment pour les événements de données appelés par d'autres comptes.	3 mars 2022

Documentation mise à jour	Cette mise à jour prend en charge la version suivante pour la bibliothèque de CloudTrail traitement : ajout de la prise en charge de la mise en œuvre d'un gestionnaire S3 personnalisé, enregistrement des événements pour enregistrer les exceptions liées à l'analyse des fichiers, prise en charge de l'analyse d'un `errorCode` champ facultatif dans `insightDetails` et mise à jour de l'identifiant de compte d'analyse régulière pour accepter des valeurs non numériques. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et de la bibliothèque CloudTrail de traitement sur GitHub.	28 janvier 2022

Fonctionnalité ajoutée	CloudTrail présente CloudTrail Lake, une nouvelle fonctionnalité qui vous permet d'exécuter des requêtes SQL précises à champs multiples sur vos événements. Les événements sont agrégés dans des magasins de données d'événement, qui sont des ensembles inaltérables d'événements basés sur des critères que vous sélectionnez en appliquant les sélecteurs d'événements avancés. Pour plus d'informations, consultez la section Travailler avec CloudTrail Lake.	5 janvier 2022
Prise en charge d'une nouvelle région	CloudTrail soutien accru à une nouvelle région, la région Asie-Pacifique (Jakarta). Pour plus d'informations, consultez la section Régions CloudTrail prises en charge.	13 décembre 2021
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon WorkSpaces Web. Consultez Intégrations et services supportés par AWS CloudTrail.	3 décembre 2021

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer CloudTrail des événements de données sur des AWS Glue tables créées par Lake Formation à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	30 novembre 2021
Fonctionnalité modifiée	En tant que bonne pratique en matière de sécurité, vous pouvez désormais ajouter une clé de `aws:SourceAccount` condition `aws:SourceArn` or aux politiques AWS KMS clés et aux politiques de compartiment Amazon S3. Pour plus d'informations, consultez Configurer les politiques AWS KMS clés CloudTrail et Configurer les politiques de compartiment Amazon S3 pour CloudTrail.	le 15 novembre 2021
Prise en charge de services supplémentaires	Cette version prend en charge AWS Resilience Hub. Consultez Intégrations et services supportés par AWS CloudTrail.	Le10 novembre 2021

Fonctionnalité ajoutée	Un nouveau type d'événement CloudTrail Insights est disponible : le taux d'erreur des événements Insights. Un événement Insights de taux d'erreur capture une activité inhabituelle sur une erreur survenant sur les API appelées dans votre compte. Pour en savoir plus, consultez Journalisation d'événements de données pour les journaux de suivi.	Le 10 novembre 2021
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de CloudTrail données sur les flux DynamoDB à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	22 septembre 2021
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de données sur les points d'accès Amazon S3. Vous pouvez enregistrer les événements de données de point d'accès Amazon S3 à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	24 août 2021

Fonctionnalité modifiée	Lorsque vous configurez un suivi pour envoyer des notifications à Amazon SNS, vous ajoutez une déclaration CloudTrail de politique à votre politique d'accès aux rubriques SNS qui permet d'envoyer du contenu CloudTrail à une rubrique SNS. Pour des raisons de sécurité, nous vous recommandons d'ajouter une clé de `aws:SourceAccount` condition `aws:SourceArn` or à la déclaration CloudTrai l de politique. Pour plus d'informations, consultez la politique relative aux rubriques Amazon SNS pour. CloudTrail	16 août 2021
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Route 53 Applicati on Recovery Controller. Consultez Intégrations et services supportés par AWS CloudTrail.	27 Juillet 2021

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de données sur les API directes Amazon EBS exécutées sur des instantanés EBS. Vous pouvez enregistrer les événements de données API directes Amazon EBS à l'aide de sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	27 Juillet 2021
Fonctionnalité modifiée	Lors du CloudTrail traitement des événements de données, il conserve les nombres dans leur format d'origine, qu'il s'agisse d'un entier (`int`) ou d'un`float`. Dans les événements contenant des nombres entiers dans les champs d'un événement de données, ces nombres CloudTrail étaient traditionnellement traités comme des nombres flottants. CloudTrail Conserve désormais le format original des entiers dans les événements de données. Pour plus d'informations, consultez la section Utilisation de la bibliothèque CloudTrail de traitement.	13 juillet 2021

Fonctionnalité ajoutée	Vous pouvez désormais exclure les événements de gestion de l'API de données Amazon RDS de vos pistes. Pour plus d'informations, consultez Journalisation des événements de gestion pour les journaux de suivi.	1er juillet 2021
Prise en charge de services supplémentaires	Cette version prend en charge AWS BugBust. Consultez Intégrations et services supportés par AWS CloudTrail.	24 juin 2021
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Managed Grafana et Amazon Managed Service for Prometheus. Consultez Intégrations et services supportés par AWS CloudTrail.	2 juin 2021
Prise en charge de services supplémentaires	Cette version est compatible avec AWS App Runner. Consultez Intégrations et services supportés par AWS CloudTrail.	18 mai 2021
Prise en charge de services supplémentaires	Cette version prend en charge AWS Systems Manager Incident Manager. Consultez Intégrations et services supportés par AWS CloudTrail.	10 mai 2021

Documentation mise à jour	Cette mise à jour décrit les exigences d'enregistrement des événements de données pour les packs de AWS Config conformité, en particulier pour les cadres de conformité tels que HIPAA ou FedRAMP. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	7 mai 2021
Prise en charge de services supplémentaires	Cette version prend en charge Service Quotas et les API directes Amazon EBS. Consultez Intégrations et services supportés par AWS CloudTrail.	13 avril 2021
Fonctionnalité ajoutée	Une fois qu'un administrateur IAM a configuré AWS STS, enregistré CloudTrail des `sourceIdentity` informations dans des événements lorsque les utilisateurs assument un rôle IAM ou exécutent des actions avec le rôle assumé. Pour en savoir plus, consultez Élément CloudTrail userIdentity.	13 avril 2021

Documentation mise à jour	Cette mise à jour décrit les limites, en kilo-octets (Ko), du contenu de certains champs d'enregistrement d' CloudTrai lévénements. Pour plus d'informations, consultez la section Contenu des CloudTrai l enregistrements.	08 avril 2021
Fonctionnalités ajoutées	Une fois qu'un administrateur IAM a configuré AWS STS, enregistré CloudTrail des `sourceIdentity` informati ons dans des événement s lorsque les utilisateurs assument un rôle IAM ou exécutent des actions avec le rôle assumé. Pour en savoir plus, consultez Élément CloudTrail userIdentity.	6 avril 2021
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événement s de données sur les tables Amazon DynamoDB. Vous pouvez enregistrer les événements de données DynamoDB à l'aide de sélecteurs d'événements ou de sélecteurs d'événements avancés. Pour plus d'informa tions, veuillez consulter Journalisation des événement s de données.	23 mars 2021

Prise en charge de services supplémentaires	Cette version prend en charge Amazon Managed Workflows for Apache Airflow Consultez Intégrations et services supportés par AWS CloudTrail.	22 mars 2021
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de données sur les points d'accès S3 Object Lambda si vous avez choisi d'utiliser des sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	18 mars 2021
Prise en charge de services supplémentaires	Cette version prend en charge le simulateur d'injection de AWS défauts. Consultez Intégrations et services supportés par AWS CloudTrail.	15 mars 2021
Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événements de données sur les nœuds Ethereum dans Amazon Managed Blockchain si vous avez choisi d'utiliser des sélecteurs d'événements avancés. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	1er mars 2021

Prise en charge de services supplémentaires	Cette version prend en charge Amazon Managed Blockchain et l'aperçu d'Ethereum for Managed Blockchain. Consultez Intégrations et services supportés par AWS CloudTrail.	4 février 2021
Prise en charge de services supplémentaires	Cette version prend en charge AWS Amplify. Consultez Intégrations et services supportés par AWS CloudTrail.	3 février 2021
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Lookout for Metrics. Consultez Intégrations et services supportés par AWS CloudTrail.	1er février 2021
Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque de CloudTrail traitement : mettez à jour les références au fichier .jar dans le guide de l'utilisateur pour utiliser la dernière version, aws-cloudtrail-processing-library -1.4.0.jar. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et de la bibliothèque CloudTrail de traitement sur GitHub.	12 janvier 2021

Fonctionnalité ajoutée	Vous pouvez désormais enregistrer les événement s de données sur Amazon S3 sur AWS Outposts. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	21 décembre 2020
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Lookout for Equipment AWS Well-Architected Tool et Amazon Location Service. Consultez Intégrations et services supportés par AWS CloudTrai l.	16 décembre 2020
Prise en charge de services supplémentaires	Cette version prend en charge la AWS IoT Greengrass V2. Consultez Intégrations et services supportés par AWS CloudTrail.	15 décembre 2020
Prise en charge de services supplémentaires	Cette version prend en charge Amazon EMR sur EKS. Consultez Intégrations et services supportés par AWS CloudTrail.	10 décembre 2020
Prise en charge de services supplémentaires	Cette version prend en charge AWS Audit Manager et Amazon HealthLake. Consultez Intégrations et services supportés par AWS CloudTrail.	8 décembre 2020

Prise en charge de services supplémentaires	Cette version prend en charge Amazon Lookout for Vision. Consultez Intégrations et services supportés par AWS CloudTrail.	1er décembre 2020
Fonctionnalité ajoutée	La version de l' AWS CloudTrail événement est désormais 1.08. La version 1.08 introduit de nouveaux champs pour CloudTrail. Pour plus d'informations, consultez la section Contenu des CloudTrail enregistrements.	24 novembre 2020
Fonctionnalité ajoutée	AWS CloudTrail introduit des sélecteurs d'événements avancés pour les événements de données. Les sélecteurs d'événements avancés permettent de contrôler les événements de données que vous vous connectez à votre piste. Vous pouvez inclure ou exclure des événements de données pour des AWS ressources spécifiques, et sélectionner des API spécifiques sur ces ressources pour vous connecter à votre historique. Pour plus d'informations, veuillez consulter Journalisation des événements de données.	24 novembre 2020

Prise en charge de services supplémentaires	Cette version prend en charge AWS Network Firewall. Consultez Intégrations et services supportés par AWS CloudTrail.	17 novembre 2020
Prise en charge de services supplémentaires	Cette version est compatible avec AWS Trusted Advisor. Consultez Intégrations et services supportés par AWS CloudTrail.	22 octobre 2020
Documentation mise à jour	Ajout de deux nouveaux exemples d'enregistrements d'événements pour les événements de connexion utilisateur racine. Pour plus d'informations, consultez Événements de connexion à la console AWS.	13 octobre 2020
Fonctionnalité modifiée	Autorisations de la politique `AWSCloudTrail_FullAccess` a été restreinte. Cette politique ne vous permet plus de supprimer des rubriques Amazon SNS ou des compartiments Amazon S3, et le `getObject` a été supprimé. Pour plus d'informations, consultez la section Octroi d'autorisations personnalisées aux CloudTrail utilisateurs.	29 septembre 2020

Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque de CloudTrail traitement : mettez à jour les références au fichier .jar dans le guide de l'utilisateur pour utiliser la dernière version, aws-cloud trail-processing-library -1.3.0.ja r. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et de la bibliothèque CloudTrail de traitement sur GitHub.	28 août 2020
Prise en charge de services supplémentaires	Cette version prend en charge AWS Outposts. Consultez Intégrations et services supportés par AWS CloudTrai l.	28 août 2020

Fonctionnalité ajoutée	AWS CloudTrail Insights introduit des champs d'attribution pour les événements CloudTrail Insights. Les champs d'attribution affichent les identités utilisateur, les agents utilisateur et les codes d'erreur les plus importants associés à l'activité anormale qui déclenche les événements Insights. À des fins de comparaison, les champs d'attribution affichent également les identités utilisateur, les agents utilisateur et les codes d'erreur les plus importants associés à une activité normale ou planifiée. Pour plus d'informations, consultez Consignation d'événements de données pour les journaux de suivi.	13 août 2020
Fonctionnalité ajoutée	La AWS CloudTrail console a un nouveau look conçu pour en faciliter l'utilisation. Le guide de AWS CloudTrail l'utilisateur a été mis à jour avec des modifications apportées aux procédures relatives à l'exécution des tâches dans la console, telles que la création de traces, la mise à jour de pistes et le téléchargement de l'historique des événements.	13 août 2020

Prise en charge de services supplémentaires	Note de mise à jour Amazon Interactive Video Service Consultez Intégrations et services supportés par AWS CloudTrail.	15 juillet 2020
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Honeycode . Consultez Intégrations et services supportés par AWS CloudTrail.	24 juin 2020
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Macie. Consultez Intégrations et services supportés par AWS CloudTrail.	19 mai 2020
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Kendra. Consultez Intégrations et services supportés par AWS CloudTrail.	13 mai 2020
Prise en charge de services supplémentaires	Cette version prend en charge AWS IoT SiteWise. Consultez Intégrations et services supportés par AWS CloudTrail.	29 avril 2020
Ajout de support de région	Cette version prend en charge une région supplémentaire : Europe (Milan). Consultez Régions compatibles avec AWS CloudTrail.	28 avril 2020

Ajout du service et de la prise en charge de la région	Cette version est compatible avec Amazon AppFlow. Consultez Intégrations et services supportés par AWS CloudTrail. Un Support a été ajouté à la région Afrique (Le Cap). Consultez Régions compatibles avec AWS CloudTrail.	22 avril 2020
Fonctionnalité ajoutée	Les AWS KMS actions à volume élevé`Encrypt`, telles que, et`Decrypt`, `GenerateDataKey` sont désormais enregistrées en tant qu'événements de lecture. Si vous choisissez d'enregistrer tous les AWS KMS événements de votre parcours, et que vous choisissez également de consigner les événements de gestion Write, votre parcours enregistre les AWS KMS actions pertinentes telles que`Disable`, `Delete` et`ScheduleKey` .	7 avril 2020
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon CodeGuru Reviewer. Consultez Intégrations et services supportés par AWS CloudTrail.	7 février 2020

Prise en charge de services supplémentaires	Cette version prend en charge le service Amazon Managed Apache Cassandra. Consultez Intégrations et services supportés par AWS CloudTrail.	17 janvier 2020
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Connect. Consultez Intégrations et services supportés par AWS CloudTrail.	13 décembre 2019
Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque de CloudTrail traitement : mettez à jour les références au fichier .jar dans le guide de l'utilisateur pour utiliser la dernière version, aws-cloud trail-processing-library -1.2.0.jar. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et de la bibliothèque CloudTrail de traitement sur GitHub.	21 novembre 2019
Fonctionnalité ajoutée	Cette version intègre AWS CloudTrail Insights pour vous aider à détecter les activités inhabituelles sur votre compte. Consultez Journalisation des événements Insights pour les journaux de suivi.	20 novembre 2019

Fonctionnalité ajoutée	Cette version ajoute une option permettant de filtrer les AWS Key Managemen t Service événements hors d'une piste. Consultez Création d'un journal de suivi.	20 novembre 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS CodeStar les notificat ions. Consultez Intégrations et services supportés par AWS CloudTrail.	7 novembre 2019
Fonctionnalité ajoutée	Cette version prend en charge l'ajout de balises lorsque vous créez un trail CloudTrail, que vous utilisiez la CloudTrail console ou l'API. Cette version ajoute deux nouvelles API, `GetTrail` et `ListTrails` .	1er novembre 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS App Mesh. Consultez Intégrations et services supportés par AWS CloudTrai l.	17 octobre 2019
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Translate. Consultez Intégrations et services supportés par AWS CloudTrai l.	17 octobre 2019

Mise à jour de la documentation	La rubrique Services non pris en charge a été restaurée et mise à jour pour inclure uniquement les AWS services qui ne connectent pas actuellement les CloudTrail événements. Consultez Services non pris en charge par CloudTrail .	7 octobre 2019
Mise à jour de la documentation	La documentation a été mise à jour pour refléter les modifications apportées à la politique `AWSCloudTrailFullAccess` . Un exemple de politique qui montre des autorisations équivalentes à `AWSCloudTrailFullAccess` a été mis à jour pour limiter les ressources sur lesquelles l'action `iam:PassRole` peut agir sur celles qui correspondent à la déclaration de condition suivante : `"iam:PassedToService": "cloudtrail.amazonaws.com"` . Consultez Exemples de politique AWS CloudTrail basée sur l'identité.	24 septembre 2019

Mise à jour de la documentation	La documentation a été mise à jour avec une nouvelle rubrique, Gestion des CloudTrail coûts, pour vous aider à obtenir les données de journal dont vous avez besoin CloudTrail tout en respectant votre budget.	3 septembre 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS Control Tower. Consultez Intégrations et services supportés par AWS CloudTrail.	13 août 2019
Ajout de support de région	Cette version prend en charge une région supplémentaire : Moyen-Orient (Bahreïn). Consultez Régions compatibles avec AWS CloudTrail.	29 juillet 2019
Mise à jour de la documentation	La documentation a été mise à jour avec des informations sur la sécurité pour CloudTrail. Consultez la section Sécurité dans AWS CloudTrail.	3 juillet 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS Ground Station. Consultez Intégrations et services supportés par AWS CloudTrail.	6 juin 2019

Prise en charge de services supplémentaires	Cette version prend en charge AWS IoT Things Graph. Consultez Intégrations et services supportés par AWS CloudTrail.	4 juin 2019
Prise en charge de services supplémentaires	Cette version prend en charge Amazon AppStream 2.0. Consultez Intégrations et services supportés par AWS CloudTrail.	25 avril 2019
Ajout de support de région	Cette version prend en charge une région supplémentaire : Asie-Pacifique (Hong Kong). Consultez Régions compatibles avec AWS CloudTrail.	24 avril 2019
Prise en charge de services supplémentaires	Cette version prend en charge le service géré Amazon pour Apache Flink. Consultez Intégrations et services supportés par AWS CloudTrail.	22 mars 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS Backup. Consultez Intégrations et services supportés par AWS CloudTrail.	4 février 2019
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon WorkLink. Consultez Intégrations et services supportés par AWS CloudTrail.	23 janvier 2019

Prise en charge de services supplémentaires	Cette version prend en charge AWS Cloud9. Consultez Intégrations et services supportés par AWS CloudTrail.	21 janvier 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS Elemental MediaLive. Consultez Intégrations et services supportés par AWS CloudTrail.	19 janvier 2019
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Comprehend. Consultez Intégrations et services supportés par AWS CloudTrail.	18 janvier 2019
Prise en charge de services supplémentaires	Cette version prend en charge AWS Elemental MediaPackage. Consultez Intégrations et services supportés par AWS CloudTrail.	21 décembre 2018
Ajout de support de région	Cette version prend en charge une région supplémentaire : EU (Stockholm). Consultez Régions compatibles avec AWS CloudTrail.	11 décembre 2018
Mise à jour de la documentation	La documentation a été mise à jour avec les informations sur les services pris en charge et non pris en charge. Consultez Intégrations et services supportés par AWS CloudTrail.	3 décembre 2018

Prise en charge de services supplémentaires	Cette version prend en charge le AWS Resource Access Manager (AWS RAM). Consultez Intégrations et services supportés par AWS CloudTrail.	20 novembre 2018
Fonctionnalités mises à jour	Cette version prend en charge la création d'un journal CloudTrail qui enregistre les événements pour tous les AWS comptes d'une organisation dans AWS Organizations. Consultez Création d'un journal de suivi pour une organisation.	19 novembre 2018
Prise en charge de services supplémentaires	Cette version prend en charge l'API Amazon Pinpoint SMS and Voice. Consultez Intégrations et services supportés par AWS CloudTrail.	16 novembre 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS IoT Greengrass. Consultez Intégrations et services supportés par AWS CloudTrail.	29 octobre 2018

Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque de CloudTrail traitement : mettez à jour les références au fichier .jar dans le guide de l'utilisateur pour utiliser la dernière version, aws-cloud trail-processing-library -1.1.3.ja r. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et de la bibliothèque CloudTrail de traitement sur GitHub.	18 octobre 2018
Fonctionnalité ajoutée	Cette version prend en charge l'utilisation de filtres supplémentaires dans Historique des événements. Consultez la section Affichage CloudTrail des événements dans la CloudTrail console.	18 octobre 2018
Fonctionnalité ajoutée	Cette version prend en charge Amazon Virtual Private Cloud (Amazon VPC) pour établir une connexion privée entre votre VPC et AWS CloudTrail. Voir Utilisation AWS CloudTrai l avec les points de terminais on VPC d'interface.	9 août 2018
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Data Lifecycle Manager. Consultez Intégrati ons et services supportés par AWS CloudTrail.	24 juillet 2018

Prise en charge de services supplémentaires	Cette version prend en charge Amazon MQ. Consultez Intégrations et services supportés par AWS CloudTrail.	19 juillet 2018
Prise en charge de services supplémentaires	Cette version prend en charge la CLI AWS mobile. Consultez Intégrations et services supportés par AWS CloudTrail.	29 juin 2018
AWS CloudTrail notification de l'historique de la documentation disponible via le flux RSS	Vous pouvez désormais recevoir des notifications concernant les mises à jour de la AWS CloudTrail documentation en vous abonnant à un flux RSS.	29 juin 2018

Mises à jour antérieures

Le tableau suivant décrit l'historique des publications de documentation AWS CloudTrail antérieures au 29 juin 2018.

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge Amazon RDS Performance Insights. Pour plus d'informations, consultez la section Services et intégrations CloudTrail pris en charge.	21 juin 2018
Fonctionnalité ajoutée	Cette version prend en charge l'enregistrement CloudTrail de tous les événements de gestion dans l'historique des événements. Pour plus d'informations,	14 juin 2018

Modification	Description	Date de parution
	consultez Utilisation de l'historique des CloudTrail événements.	
Prise en charge de services supplémentaires	Cette version prend en charge AWS Billing and Cost Management. Consulter CloudTrail services et intégrations pris en charge.	7 juin 2018
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consulter CloudTrail services et intégrations pris en charge.	5 juin 2018
Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque CloudTrail de traitement : • Mettez à jour les références du fichier .jar dans le guide de l'utilisateur pour utiliser la dernière version, aws-cloudtrail-processing-library -1.1.2.jar. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et la bibliothèque CloudTrail de traitement sur GitHub.	16 mai 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS Billing and Cost Management. Consulter CloudTrail services et intégrations pris en charge.	7 juin 2018
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consulter CloudTrail services et intégrations pris en charge.	5 juin 2018

Modification	Description	Date de parution
Documentation mise à jour	Cette mise à jour prend en charge la version de correctif suivante pour la bibliothèque CloudTrail de traitement : • Mettez à jour les références du fichier .jar dans le guide de l'utilisateur pour utiliser la dernière version, aws-cloudtrail-processing-library -1.1.2.jar. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et la bibliothèque CloudTrail de traitement sur GitHub.	16 mai 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS X-Ray. Consulter CloudTrail services et intégrations pris en charge.	25 avril 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS IoT Analytics. Consulter CloudTrail services et intégrations pris en charge.	23 avril 2018
Prise en charge de services supplémentaires	Cette version prend en charge Secrets Manager. Consulter CloudTrail services et intégrations pris en charge.	10 avril 2018
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Rekognition. Consulter CloudTrail services et intégrations pris en charge.	6 avril 2018
Prise en charge de services supplémentaires	Cette version prend en charge l'autorité de certification AWS privée (PCA). Consulter CloudTrail services et intégrations pris en charge.	4 avril 2018

Modification	Description	Date de parution
Fonctionnalité ajoutée	Cette version permet de faciliter la recherche dans les fichiers CloudTrail journaux avec Amazon Athena. Vous pouvez créer automatiquement des tables pour interroger les journaux directement depuis la CloudTrail console et utiliser ces tables pour exécuter des requêtes dans Athena. Pour plus d'informations, consultez CloudTrail services et intégrations pris en charge la section Création d'une table pour CloudTrail les journaux dans la CloudTrail console.	15 mars 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS AppSync. Consulter CloudTrail services et intégrations pris en charge.	13 février 2018
Prise en charge de régions supplémentaires	Cette version prend en charge une région supplémentaire : Asie-Pacifique (Osaka) (ap-northeast-3). Consulter CloudTrail Régions prises en charge.	12 février 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS Shield. Consulter CloudTrail services et intégrations pris en charge.	12 février 2018
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon SageMaker . Consulter CloudTrail services et intégrations pris en charge.	11 janvier 2018
Prise en charge de services supplémentaires	Cette version prend en charge AWS Batch. Consulter CloudTrail services et intégrations pris en charge.	10 janvier 2018
Fonctionnalité ajoutée	Cette version permet d'étendre à 90 jours le volume d'activité du compte disponible dans l'historique des CloudTrail événements. Vous pouvez également personnaliser l'affichage des colonnes pour améliorer l'affichage de vos CloudTrail événements. Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.	12 décembre 2017

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon WorkMail. Consulter CloudTrail services et intégrations pris en charge.	12 décembre 2017
Prise en charge de services supplémentaires	Cette version est compatible avec Alexa for Business, AWS Elemental MediaConvert, et AWS Elemental MediaStore. Consulter CloudTrail services et intégrations pris en charge.	1er décembre 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge la journalisation des événements de données pour AWS Lambda les fonctions. Pour plus d'informations, consultez Journalisation des événements de données.	30 novembre 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge la journalisation des événements de données pour AWS Lambda les fonctions. Pour plus d'informations, consultez Journalisation des événements de données.	30 novembre 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge les mises à jour suivantes de la bibliothèque CloudTrail de traitement : • Ajout de la prise en charge de l'identification booléenne des événements de gestion. • Mettez à jour la version de l' CloudTrail événement vers la version 1.06. Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et la bibliothèque CloudTrail de traitement sur GitHub.	30 novembre 2017

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge AWS Glue. Consulter CloudTrail services et intégrations pris en charge.	7 novembre 2017
Nouvelle documentation	Cette version ajoute une nouvelle rubrique, Quotas dans AWS CloudTrail.	19 octobre 2017
Documentation mise à jour	Cette version met à jour la documentation des API prises en charge dans l'historique des CloudTrail événements pour Amazon Athena, AWS CodeBuild Amazon Elastic Container Registry et. AWS Migration Hub	13 octobre 2017
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Chime. Consulter CloudTrail services et intégrations pris en charge.	27 septembre 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge la configuration de la journalisation des événements de données pour tous les compartiments Amazon S3 de votre AWS compte. Consulter Journalisation des événements de données.	20 septembre 2017
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Lex. Consulter CloudTrail services et intégrations pris en charge.	15 août 2017
Prise en charge de services supplémentaires	Cette version prend en charge AWS Migration Hub. Consulter CloudTrail services et intégrations pris en charge.	14 août 2017

Modification	Description	Date de parution
Documentation et fonctionnalités supplémentaires	Cette version prend CloudTrail en charge l'activation par défaut pour tous les AWS comptes. Les sept derniers jours d'activité du compte sont disponibles dans l'historique des CloudTrail événements, et les événements les plus récents apparaissent sur le tableau de bord de la console. La fonction appelée précédemment API activity history (Historique d'activité de l'API) a été remplacée par Event history (Historique des événements).	14 août 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge le téléchargement d'événements depuis la CloudTrail console sur la page d'historique des activités de l'API. Vous pouvez télécharger les événements au format JSON ou CSV. Pour plus d'informations, consultez Téléchargement des événements.	27 juillet 2017
Fonctionnalité ajoutée	Cette version prend en charge la journalisation des opérations d'API au niveau des objets Amazon S3 dans deux régions supplémentaires, Europe (Londres) et Canada (Centre). Pour plus d'informations, consultez Utilisation de fichiers CloudTrail journaux.	19 juillet 2017
Prise en charge de services supplémentaires	Cette version prend en charge la recherche d'API pour Amazon CloudWatch Events dans la fonctionnalité d'historique des activités des CloudTrail API.	27 juin 2017

Modification	Description	Date de parution
Documentation et fonctionnalités supplémentaires	Cette version prend en charge des API supplémentaires dans la fonctionnalité d'historique des activités des CloudTrail API pour les services suivants : • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	27 juin 2017
Prise en charge de services supplémentaires	Cette version prend en charge AWS CodeStar. Consulter CloudTrail services et intégrations pris en charge.	14 juin 2017

Modification	Description	Date de parution

Documentation et fonctionnalités supplémentaires	Cette version prend en charge les mises à jour suivantes de la bibliothèque CloudTrail de traitement :
	• Ajoutez la prise en charge de différents formats pour les messages SQS provenant de la même file d'attente SQS afin d'identifier les fichiers CloudTrail journaux. Les formats suivants sont pris en charge :
	  • Notifications CloudTrail envoyées à une rubrique SNS
	  • Notifications envoyées par Amazon S3 à une rubrique SNS
	  • Notifications envoyées par Amazon S3 directement à une file d'attente SQS
	• Ajout de la prise en charge de la propriété `deleteMessageUponFailure` , que vous pouvez utiliser pour supprimer les messages qui ne peuvent pas être traités.
	
	Pour plus d'informations, voir Utilisation de la bibliothèque CloudTrail de traitement et la bibliothèque CloudTrail de traitement sur GitHub.
		1er juin 2017

Prise en charge de services supplémentaires	Cette version prend en charge Amazon Athena. Consulter CloudTrail services et intégrations pris en charge.	19 mai 2017

Modification	Description	Date de parution
Fonctionnalité ajoutée	Cette version prend en charge l'envoi d'événements de données à Amazon CloudWatch Logs. Pour plus d'informations sur la configuration de votre journal de suivi pour la consignation des événements de données, consultez Événements de données. Pour plus d'informations sur l'envoi d'événements à CloudWatch Logs, consultezSurveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.	9 mai 2017
Prise en charge de services supplémentaires	Cette version prend en charge le AWS Marketplace service de mesure. Consulter CloudTrail services et intégrations pris en charge.	2 mai 2017
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon QuickSigh t. Consulter CloudTrail services et intégrations pris en charge.	28 avril 2017
Documentation et fonctionnalités supplémen taires	Cette version prend en charge une expérience de console mise à jour pour la création de journaux de suivi. Vous pouvez désormais configurer un nouveau journal de suivi pour consigner les événements de gestion et de données. Pour plus d'informations, consultez Création d'un journal de suivi.	11 avril 2017

Modification	Description	Date de parution
Ajout de documentation	CloudTrail S'il ne fournit pas de journaux à votre compartiment S3 ou n'envoie pas de notifications SNS depuis certaines régions de votre compte, vous devrez peut-être mettre à jour les politiques. Pour en savoir plus sur la mise à jour de votre politique de compartiment S3, consultez Erreurs courantes de configuration de politique Amazon S3. Pour en savoir plus sur la mise à jour de votre politique de rubrique SNS, consultez CloudTrail n'envoie pas de notifications pour une région.	31 mars 2017
Prise en charge de services supplémentaires	Cette version prend en charge AWS Organizations. Consulter CloudTrail services et intégrations pris en charge.	27 février 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge une expérience de console mise à jour pour la configuration de journaux de suivi pour la journalisation des événements de gestion et de données. Pour plus d'informations, consultez Utilisation de fichiers CloudTrail journaux.	10 février 2017
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Cloud Directory. Consulter CloudTrail services et intégrations pris en charge.	26 janvier 2017
Documentation et fonctionnalités supplémentaires	Cette version permet de rechercher des API pour AWS CodeCommit Amazon GameLift et AWS Managed Services dans l'historique des activités des CloudTrail API.	26 janvier 2017

Modification	Description	Date de parution
Fonctionnalité ajoutée	Cette version prend en charge l'intégration à l' AWS Health Dashboard. Vous pouvez utiliser le AWS Health Dashboard pour déterminer si vos sentiers ne sont pas en mesure de fournir des journaux à une rubrique SNS ou à un compartiment S3. Cela peut se produire en cas de problème avec la politique du compartiment S3 ou du sujet SNS. AWS Health Dashboard vous informe des sentiers concernés et vous recommande des moyens de corriger la politique. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Health.	24 janvier 2017
Documentation et fonctionnalités supplémentaires	Cette version prend en charge le filtrage par source d'événement dans la CloudTrail console. La source de l'événement indique le AWS service auquel la demande a été adressée. Pour plus d'informations, consultez Afficher les événements de gestion récents à l'aide de la console.	12 janvier 2017
Prise en charge de services supplémentaires	Cette version prend en charge AWS CodeCommit. Consulter CloudTrail services et intégrations pris en charge.	11 janvier 2017
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Lightsail. Consulter CloudTrail services et intégrations pris en charge.	23 décembre 2016
Prise en charge de services supplémentaires	Cette version prend en charge les AWS Managed Services. Consultez CloudTrail services et intégrations pris en charge.	21 décembre 2016

Modification	Description	Date de parution
Prise en charge de régions supplémentaires	Cette version prend en charge la région Europe (Londres). Consultez CloudTrail Régions prises en charge.	13 décembre 2016
Prise en charge de régions supplémentaires	Cette version prend en charge la région Canada (Centre). Consultez CloudTrail Régions prises en charge.	8 décembre 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS CodeBuild SeeCloudTrail services et intégrations pris en charge. Cette version prend en charge AWS Health. veuillez consulter CloudTrail services et intégrations pris en charge. Cette version prend en charge AWS Step Functions. Consultez CloudTrail services et intégrations pris en charge.	1er décembre 2016
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Polly. Consultez CloudTrail services et intégrations pris en charge.	30 novembre 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS OpsWorks for Chef Automate. Consultez CloudTrail services et intégrations pris en charge.	23 novembre 2016

Modification	Description	Date de parution
Documentation et fonctionnalités supplémentaires	Cette version prend en charge la configuration de votre journal de suivi pour journaliser des événements en lecture seule, en écriture seule, ou tous les événements. CloudTrail prend en charge la journalisation des opérations d'API au niveau des objets Amazon S3 `GetObject`, telles que `PutObject`, et `DeleteObject`. Vous pouvez configurer vos journaux de suivi pour journaliser les opérations d'API au niveau de l'objet. Pour plus d'informations, consultez Utilisation de fichiers CloudTrail journaux.	21 novembre 2016
Documentation et fonctionnalités supplémentaires	Cette version prend en charge des valeurs supplémentaires pour le champ `type` de l'élément `userIdentity` : `AWSAccount` et `AWSService`. Pour plus d'informations, consultez Champs pour `userIdentity`.	16 novembre 2016
Prise en charge de services supplémentaires	Prise en charge de la fonction Application Auto Scaling Consultez CloudTrail services et intégrations pris en charge.	31 octobre 2016
Prise en charge de régions supplémentaires	Cette version prend en charge la région USA Est (Ohio). Consultez CloudTrail Régions prises en charge.	17 octobre 2016
Documentation et fonctionnalités supplémentaires	Cette version prend en charge la journalisation des événements de AWS service non liés à l'API. Pour plus d'informations, consultez AWS événements de service.	23 septembre 2016

Modification	Description	Date de parution
Documentation et fonctionnalités supplémentaires	Cette version prend en charge l'utilisation de la CloudTrail console pour afficher les types de ressources pris en charge par AWS Config. Pour plus d'informations, consultez Affichage des ressources référencées avec AWS Config.	7 juillet 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS Service Catalog. Consultez CloudTrail services et intégrations pris en charge.	6 juillet 2016
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Elastic File System (Amazon EFS). Consultez CloudTrail services et intégrations pris en charge.	28 juin 2016
Prise en charge de régions supplémentaires	Cette version prend en charge une région supplémentaire : ap-south-1 (Asie-Pacifique [Mumbai]). Consultez CloudTrail Régions prises en charge.	27 juin 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS Application Discovery Service. Consultez CloudTrail services et intégrations pris en charge.	12 mai 2016
Prise en charge de services supplémentaires	Cette version prend en charge CloudWatch les journaux dans la région Amérique du Sud (São Paulo). Pour plus d'informations, consultez Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.	6 mai 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS WAF. Consultez CloudTrail services et intégrations pris en charge.	28 avril 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS Support. Consultez CloudTrail services et intégrations pris en charge.	21 avril 2016

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Inspector. Consultez CloudTrail services et intégrations pris en charge.	20 avril 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS IoT. Consultez CloudTrail services et intégrations pris en charge.	11 avril 2016
Documentation et fonctionnalités supplémentaires	Cette version prend en charge les appels d'API logging AWS Security Token Service (AWS STS) effectués avec le langage SAML (Security Assertion Markup Language) et la fédération d'identité Web. Pour plus d'informations, consultez Valeurs des AWS STS API avec SAML et fédération d'identité Web.	28 mars 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS Certificate Manager. Consultez CloudTrail services et intégrations pris en charge.	25 mars 2016
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon Data Firehose. Consultez CloudTrail services et intégrations pris en charge.	17 mars 2016
Prise en charge de services supplémentaires	Cette version prend en charge Amazon CloudWatch Logs. Consultez CloudTrail services et intégrations pris en charge.	10 mars 2016
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Cognito. Consultez CloudTrail services et intégrations pris en charge.	18 février 2016
Prise en charge de services supplémentaires	Cette version prend en charge AWS Database Migration Service. Consultez CloudTrail services et intégrations pris en charge.	4 février 2016

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon GameLift (Amazon GameLift). Consultez CloudTrail services et intégrations pris en charge.	27 janvier 2016
Prise en charge de services supplémentaires	Cette version prend en charge Amazon CloudWatch Events. Consultez CloudTrail services et intégrations pris en charge.	16 janvier 2016
Prise en charge de régions supplémentaires	Cette version prend en charge une autre région : ap-northeast-2 (Asie-Pacifique [Séoul]). Consultez CloudTrail Régions prises en charge.	6 janvier 2016
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Elastic Container Registry (Amazon ECR). Consultez CloudTrail services et intégrations pris en charge.	21 décembre 2015
Documentation et fonctionnalités supplémentaires	Cette version prend en charge l'activation CloudTrail dans toutes les régions et la prise en charge de plusieurs sentiers par région. Pour plus d'informations, consultez Travailler avec les CloudTrail sentiers.	17 décembre 2015
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Machine Learning. Consultez CloudTrail services et intégrations pris en charge.	10 décembre 2015
Documentation et fonctionnalités supplémentaires	Cette version prend en charge le chiffrement des fichiers journaux, la validation de l'intégrité des fichiers journaux et l'étiquetage. Pour plus d'informations, consultez Chiffrement des fichiers CloudTrail journaux à l'aide de AWS KMS clés (SSE-KMS), Validation de l' CloudTrail intégrité du fichier journal et Mise à jour d'un journal de suivi.	1er octobre 2015

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge Amazon OpenSearch Service. Consultez CloudTrail services et intégrations pris en charge.	1er octobre 2015
Prise en charge de services supplémentaires	Cette version prend en charge les événements au niveau du compartiment Amazon S3. Consultez CloudTrail services et intégrations pris en charge.	1er septembre 2015
Prise en charge de services supplémentaires	Cette version prend en charge AWS Device Farm. Consultez CloudTrail services et intégrations pris en charge.	13 juillet 2015
Prise en charge de services supplémentaires	Cette version prend en charge Amazon API Gateway. Consultez CloudTrail services et intégrations pris en charge.	9 juillet 2015
Prise en charge de services supplémentaires	Cette version prend en charge CodePipeline. Consultez CloudTrail services et intégrations pris en charge.	9 juillet 2015
Prise en charge de services supplémentaires	Cette version prend en charge Amazon DynamoDB. Consultez CloudTrail services et intégrations pris en charge.	28 mai 2015
Prise en charge de services supplémentaires	Cette version prend en charge CloudWatch les journaux dans la région de l'ouest des États-Unis (Californie du Nord). Pour plus d'informations sur la CloudTrail prise en charge de la surveillance des CloudWatch journaux, consultezSurveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs.	19 mai 2015
Prise en charge de services supplémentaires	Cette version prend en charge AWS Directory Service. Consultez CloudTrail services et intégrations pris en charge.	14 mai 2015

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Simple Email Service (Amazon SES). Consultez CloudTrail services et intégrations pris en charge.	7 mai 2015
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Elastic Container Service See CloudTrail services et intégrations pris en charge.	9 avril 2015
Prise en charge de services supplémentaires	Cette version prend en charge AWS Lambda. Consultez CloudTrail services et intégrations pris en charge.	9 avril 2015
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon WorkSpaces. Consultez CloudTrail services et intégrations pris en charge.	9 avril 2015
	Cette version prend en charge la recherche d'AWS activités capturées par CloudTrail (CloudTrail événements). Vous pouvez rechercher et filtrer les événements de votre compte liés à la création, la modification ou la suppression. Pour rechercher ces événements, vous pouvez utiliser la CloudTrail console, le AWS Command Line Interface (AWS CLI) ou le AWS SDK. Pour plus d'informations, consultez Utilisation de l'historique des CloudTrail événements.	12 mars 2015
Prise en charge de services supplémentaires et nouvelle documentation	Cette version prend en charge Amazon CloudWatch Logs dans les régions Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Asie-Pacifique (Tokyo) et Europe (Francfort). Pour plus d'informations, consultez la section Envoi d'événements aux CloudWatch journaux.	5 mars 2015

Modification	Description	Date de parution
Nouvelle documentation	Une nouvelle section qui décrit la CloudTrail prise en charge des points de terminaison régionaux AWS Security Token Service (AWS STS) a été ajoutée à la page CloudTrail Concepts.	17 février 2015
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Route 53. Consultez CloudTrail services et intégrations pris en charge.	11 février 2015
Prise en charge de services supplémentaires	Cette version prend en charge AWS Config. Consultez CloudTrail services et intégrations pris en charge.	10 février 2015
Prise en charge de services supplémentaires	Cette version prend en charge AWS CloudHSM. Consultez CloudTrail services et intégrations pris en charge.	8 janvier 2015
Prise en charge de services supplémentaires	Cette version prend en charge AWS CodeDeploy. Consultez CloudTrail services et intégrations pris en charge.	17 décembre 2014
Prise en charge de services supplémentaires	Cette version prend en charge AWS Storage Gateway. Consultez CloudTrail services et intégrations pris en charge.	16 décembre 2014
Prise en charge de régions supplémentaires	Cette version prend en charge une région supplémentaire : us-gov-west -1 (AWS GovCloud (US-West)). Consultez CloudTrail Régions prises en charge.	16 décembre 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon S3 Glacier. Consultez CloudTrail services et intégrations pris en charge.	11 décembre 2014
Prise en charge de services supplémentaires	Cette version prend en charge AWS Data Pipeline. Consultez CloudTrail services et intégrations pris en charge.	2 décembre 2014

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge AWS Key Management Service. Consultez CloudTrail services et intégrations pris en charge.	12 novembre 2014
Nouvelle documentation	Une nouvelle section, Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs, a été ajoutée au guide. Il décrit comment utiliser Amazon CloudWatch Logs pour surveiller les événements des CloudTrail journaux.	10 novembre 2014
Nouvelle documentation	Une nouvelle section, Utilisation de la bibliothèque CloudTrail de traitement, a été ajoutée au guide. Il fournit des informations sur la façon d'écrire un processeur de CloudTrail log en Java à l'aide de la bibliothèque AWS CloudTrail de traitement.	5 novembre 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Elastic Transcoder. Consultez CloudTrail services et intégrations pris en charge.	27 octobre 2014
Prise en charge de régions supplémentaires	Cette version prend en charge une autre région : eu-central-1 (). Consultez CloudTrail Régions prises en charge.	23 octobre 2014
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon CloudSearch. Consultez CloudTrail services et intégrations pris en charge.	16 octobre 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Simple Notification Service. Consultez CloudTrail services et intégrations pris en charge.	09 octobre 2014
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon ElastiCache. Consultez CloudTrail services et intégrations pris en charge.	15 septembre 2014

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon WorkDocs. Consultez CloudTrail services et intégrations pris en charge.	27 août 2014
Ajout de nouveau contenu	Cette version comprend une rubrique qui décrit la journalisation des événements de connexion. Consultez AWS Management Console événements de connexion.	24 juillet 2014
Ajout de nouveau contenu	L'élément eventVersion de cette version a été mis à niveau vers la version 1.02 et trois nouveaux champs ont été ajoutés. Consultez CloudTrail enregistrer le contenu.	18 juillet 2014
Prise en charge de services supplémentaires	Cette version prend en charge Auto Scaling (consulte z.CloudTrail services et intégrations pris en charge).	17 juillet 2014
Prise en charge de régions supplémentaires	Cette version prend en charge trois régions supplémen taires : ap-southeast-1 (Asie-Pacifique [Singapour]), ap-northeast-1 (Asie-Pacifique [Tokyo]), sa-east-1 (Amérique du Sud [São Paulo]). Consultez CloudTrail Régions prises en charge.	30 juin 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Redshift. Consultez CloudTrail services et intégrations pris en charge.	10 juin 2014
Prise en charge de services supplémentaires	Cette version prend en charge AWS OpsWorks. Consultez CloudTrail services et intégrations pris en charge.	5 juin 2014
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon CloudFron t. Consultez CloudTrail services et intégrations pris en charge.	28 mai 2014

Modification	Description	Date de parution
Prise en charge de régions supplémentaires	Cette version prend en charge trois régions supplémentaires : us-west-1 (USA Ouest [Californie du Nord]), eu-west-1 (Europe [Irlande]), ap-southeast-2 (Asie-Pacifique [Sydney]). Consultez CloudTrail Régions prises en charge.	13 mai 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Simple Workflow Service. Consultez CloudTrail services et intégrations pris en charge.	9 mai 2014
Ajout de nouveau contenu	Cette version contient des rubriques qui évoquent le partage de fichiers journaux entre plusieurs comptes. Consultez Partage de fichiers CloudTrail journaux entre AWS comptes.	2 mai 2014
Prise en charge de services supplémentaires	Cette version est compatible avec Amazon CloudWatch. Consultez CloudTrail services et intégrations pris en charge.	28 avril 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon Kinesis. Consultez CloudTrail services et intégrations pris en charge.	22 avril 2014
Prise en charge de services supplémentaires	Cette version prend en charge AWS Direct Connect. Consultez CloudTrail services et intégrations pris en charge.	11 avril 2014
Prise en charge de services supplémentaires	Cette version prend en charge Amazon EMR. Consultez CloudTrail services et intégrations pris en charge.	4 avril 2014
Prise en charge de services supplémentaires	Cette version prend en charge Elastic Beanstalk. Consultez CloudTrail services et intégrations pris en charge.	2 avril 2014

Modification	Description	Date de parution
Prise en charge de services supplémentaires	Cette version prend en charge AWS CloudFormation. Consultez CloudTrail services et intégrations pris en charge.	7 mars 2014
Nouveau guide	Cette version présente AWS CloudTrail.	13 novembre 2013

Glossaire AWS

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

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