aws

Guide de l’utilisateur

Explorateur de ressources AWS

Explorateur de ressources AWS: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est Explorateur de ressources AWS ?

Explorateur de ressources AWS est un service de recherche et de découverte de ressources. Avec Resource Explorer, vous pouvez explorer vos ressources, telles que les instances Amazon Elastic Compute Cloud, les flux Amazon Kinesis ou les tables Amazon DynamoDB, en utilisant une expérience similaire à celle d'un moteur de recherche sur Internet. Vous pouvez rechercher vos ressources à l'aide de métadonnées telles que les noms, les balises etIDs. L'explorateur de ressources est Régions AWS intégré à votre compte pour simplifier vos charges de travail interrégionales.

Resource Explorer fournit des réponses rapides à vos requêtes de recherche en utilisant des index créés et gérés par le Explorateur de ressources AWS service. Resource Explorer utilise diverses sources de données pour recueillir des informations sur les ressources de votre Compte AWS. Resource Explorer stocke ces informations dans les index que Resource Explorer peut rechercher.

> Nous voulons connaître votre avis sur cette documentation
>
> Notre objectif est de vous aider à tirer le meilleur parti de Resource Explorer. Si ce guide vous aide à le faire, faites-le nous savoir. Si le guide ne vous aide pas, nous aimerions avoir de vos nouvelles afin de résoudre le problème. Utilisez le lien Feedback qui se trouve dans le coin supérieur droit de chaque page. Cela envoie vos commentaires directement aux rédacteurs de ce guide. Nous examinons chaque soumission, à la recherche d'opportunités d'amélioration de la documentation. Merci d'avance pour votre aide !

Rubriques

Vous utilisez l'explorateur de ressources pour la première fois ?

Si vous utilisez l'explorateur de ressources pour la première fois, nous vous recommandons de commencer par lire les rubriques suivantes de la section Mise en route :

- Termes et concepts pour Resource Explorer
- Configuration de l'explorateur de ressources à l'aide de la configuration rapide

Caractéristiques de Resource Explorer

L'explorateur de ressources fournit les fonctionnalités suivantes :

- Les utilisateurs peuvent rechercher des ressources dans leur région Région AWS ou dans l'ensemble de leurs régions Compte AWS.
- Les utilisateurs peuvent utiliser des mots clés, des opérateurs de recherche et des attributs tels que des balises pour filtrer les résultats de recherche uniquement pour les ressources correspondantes.
- Lorsque les utilisateurs trouvent une ressource dans les résultats de recherche, ils peuvent accéder immédiatement à la console native de la ressource pour travailler avec cette ressource.
- Les administrateurs peuvent créer des vues qui définissent les ressources disponibles dans les résultats de recherche. Les administrateurs peuvent créer différentes vues pour différents groupes d'utilisateurs en fonction de leurs tâches, et accorder des autorisations d'accès aux vues uniquement aux utilisateurs qui en ont besoin.
- Resource Explorer, comme beaucoup d'autres Services AWS, est finalement cohérent. Resource Explorer atteint une haute disponibilité en répliquant les données sur plusieurs serveurs au sein des centres de données Amazon du monde entier. Si une demande de modification de certaines données aboutit, la modification est validée et stockée en toute sécurité. Cependant, la modification doit alors être répliquée dans Resource Explorer, ce qui peut prendre un certain temps. Par exemple, Resource Explorer trouve une ressource dans une région et la réplique dans la région qui contient l'index agrégateur du compte.

Régions prises en charge par Resource Explorer

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	resource-explorer-2.us-east-2.amazonaws.com resource-explorer-2-fips.us-east-2.amazonaws.com	HTTPS HTTPS HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
		resource-explorer-2-fips.us-east-2.api.aws	
US East (N. Virginia)	us-east-1	resource-explorer-2.us-east-1.amazonaws.com resource-explorer-2-fips.us-east-1.amazonaws.com resource-explorer-2-fips.us-east-1.api.aws	HTTPS HTTPS HTTPS
USA Ouest (Californie du Nord)	us-west-1	resource-explorer-2.us-west-1.amazonaws.com resource-explorer-2-fips.us-west-1.amazonaws.com resource-explorer-2-fips.us-west-1.api.aws	HTTPS HTTPS HTTPS
US West (Oregon)	us-west-2	resource-explorer-2.us-west-2.amazonaws.com resource-explorer-2-fips.us-west-2.amazonaws.com resource-explorer-2-fips.us-west-2.api.aws	HTTPS HTTPS HTTPS
Afrique (Le Cap)	af-south-1	resource-explorer-2.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	resource-explorer-2.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Hyderabad)	ap-south-2	resource-explorer-2.ap-south-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Jakarta)	ap-southeast-3	resource-explorer-2.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	resource-explorer-2.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	resource-explorer-2.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	resource-explorer-2.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	resource-explorer-2.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	resource-explorer-2.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	resource-explorer-2.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	resource-explorer-2.ap-northeast-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Canada (Central)	ca-central-1	resource-explorer-2.ca-central-1.amazonaws.com resource-explorer-2-fips.ca-central-1.amazonaws.com resource-explorer-2-fips.ca-central-1.api.aws	HTTPS HTTPS HTTPS
Canada Ouest (Calgary)	ca-west-1	resource-explorer-2.ca-west-1.amazonaws.com resource-explorer-2-fips.ca-west-1.amazonaws.com resource-explorer-2-fips.ca-west-1.api.aws	HTTPS HTTPS HTTPS
Europe (Francfort)	eu-central-1	resource-explorer-2.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	resource-explorer-2.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	resource-explorer-2.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	resource-explorer-2.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	resource-explorer-2.eu-west-3.amazonaws.com	HTTPS
Europe (Espagne)	eu-south-2	resource-explorer-2.eu-south-2.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	resource-explorer-2.eu-north-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Zurich)	eu-central-2	resource-explorer-2.eu-central-2.amazonaws.com	HTTPS
Israël (Tel Aviv)	il-central-1	resource-explorer-2.il-central-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	resource-explorer-2.me-south-1.amazonaws.com	HTTPS
Moyen-Orient (UAE)	me-central-1	resource-explorer-2.me-central-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	resource-explorer-2.sa-east-1.amazonaws.com	HTTPS

Relié Services AWS

Voici les autres Services AWS dont l'objectif principal est de vous aider à gérer vos AWS ressources :

AWS Resource Access Manager (AWS RAM)

Partagez les ressources de l'un Compte AWS avec l'autre Comptes AWS. Si votre compte est géré par AWS Organizations, vous pouvez l'utiliser AWS RAM pour partager des ressources avec les comptes d'une unité organisationnelle ou avec tous les comptes de l'organisation. Les ressources partagées fonctionnent pour les utilisateurs de ces comptes comme elles le feraient si elles avaient été créées dans le compte local.

AWS Resource Groups

Créez des groupes pour vos AWS ressources. Vous pouvez ensuite utiliser et gérer chaque groupe en tant qu'unité au lieu de devoir référencer chaque ressource individuellement. Vos groupes peuvent être composés de ressources qui font partie de la même AWS CloudFormation

pile ou qui sont étiquetées avec les mêmes balises. Certains types de ressources prennent également en charge l'application d'une configuration à un groupe de ressources afin d'affecter toutes les ressources pertinentes de ce groupe.

L'éditeur de balises et le AWS Resource Groups Tagging API

Les balises sont des métadonnées définies par le client que vous pouvez associer à vos ressources. Vous pouvez classer vos ressources à des fins telles que la répartition des coûts et le contrôle d'accès basé sur les attributs.

Tarification

La recherche de ressources en les utilisant Explorateur de ressources AWS, notamment en créant des vues, en activant des régions ou en recherchant des ressources, est gratuite. Au cours du processus de création de votre inventaire de ressources, Resource Explorer appelle APIs en votre nom, ce qui peut entraîner des frais. L'interaction avec les ressources que vous trouvez dans les résultats de recherche peut entraîner des frais d'utilisation qui varient en fonction du type de ressource et de son contenu Service AWS. Pour plus d'informations sur le AWS mode de facturation pour l'utilisation normale d'un type de ressource spécifique, reportez-vous à la documentation du service propriétaire de ce type de ressource.

Commencer à utiliser Resource Explorer

Utilisez les rubriques de cette section pour acquérir une compréhension de base des concepts et termes utilisés par Explorateur de ressources AWS. Découvrez les conditions préalables que vous devez remplir pour utiliser correctement l'explorateur de ressources et comment activer l'explorateur de ressources dans votre Compte AWS.

Accéder à l'explorateur de ressources

Vous pouvez interagir avec l'explorateur de ressources de la manière suivante :

Console Explorateur de ressources

L'explorateur de ressources fournit une interface utilisateur basée sur le web, la console Explorateur de ressources. Si vous vous êtes inscrit à un Compte AWS, vous pouvez accéder à la console Resource Explorer en vous connectant à Resource Explorer AWS Management Consoleet en choisissant Resource Explorer sur la page d'accueil de la console.

Vous pouvez également accéder directement à la page du tableau de bord de l'explorateur de ressources ou à la page de recherche de ressources dans votre navigateur. Si vous n'êtes pas encore connecté, vous êtes invité à le faire avant que la console n'apparaisse.

> **Note**
>
> La console Resource Explorer est une console globale, ce qui signifie que vous n'avez pas à en sélectionner une Région AWS pour travailler. Toutefois, lorsque vous utilisez l'Explorateur de ressources pour créer un index ou une vue, vous devez spécifier dans quelle région l'index ou la vue est stocké. Lorsque vous utilisez l'Explorateur de ressources pour effectuer une recherche, vous pouvez choisir n'importe quelle vue à laquelle vous avez accès. Les résultats proviennent automatiquement de la région associée à la vue sélectionnée. Si la vue provient de la région qui contient l'index agrégateur, les résultats incluent les ressources de toutes les régions dans lesquelles vous avez créé des index Resource Explorer.

AWS Management Console recherche unifiée

En haut de chaque page du AWS Management Console, il y a une barre de recherche. Vous pouvez configurer Resource Explorer pour participer à une recherche unifiée. Vos utilisateurs peuvent ensuite utiliser la syntaxe des requêtes de recherche de Resource Explorer dans la zone de texte de recherche unifiée et voir les ressources correspondantes dans les résultats de recherche. En activant cette fonctionnalité, les utilisateurs peuvent rechercher des ressources depuis la console de n'importe quelle console Service AWS sans avoir à passer d'abord à la console Resource Explorer.

> **Important**
>
> La recherche unifiée utilise toujours la vue par défaut dans le Région AWS qui contient l'index de l'agrégateur.

Commandes de l'explorateur de ressources dans AWS CLI et dans les outils pour Windows PowerShell

Les outils AWS CLI et pour PowerShell fournir un accès direct aux API opérations publiques de Resource Explorer. Ces outils fonctionnent sous Windows, macOS et Linux. Pour plus d'informations sur la mise en route, consultez le guide de AWS Command Line Interface l'utilisateur ou le guide de AWS Tools for Windows PowerShell l'utilisateur. Pour plus d'informations sur les commandes de Resource Explorer, consultez la référence des commandes ou la référence des AWS Tools for Windows PowerShell applets de AWS CLI commande.

Opérations de l'explorateur de ressources dans AWS SDKs

AWS fournit des API commandes pour un large éventail de langages de programmation. Pour plus d'informations sur comment démarrer, consultez Utilisation Explorateur de ressources AWS avec un AWS SDK.

Requête API

Si vous n'utilisez aucun des langages de programmation pris en charge, la HTTPS requête Resource Explorer vous API donne un accès programmatique à Resource Explorer. Avec l'explorateur de ressourcesAPI, vous pouvez HTTPS envoyer des demandes directement au service. Lorsque vous utilisez l'explorateur de ressourcesAPI, vous devez inclure un code permettant de signer numériquement vos demandes à l'aide de vos AWS informations d'identification. Pour plus d'informations, consultez la Explorateur de ressources AWS APIréférence.

Termes et concepts pour Resource Explorer

Explorateur de ressources AWS est un service de recherche et de découverte de ressources. Avec Resource Explorer, vous pouvez explorer vos ressources à l'aide d'une expérience semblable à celle d'un moteur de recherche Internet. Vous pouvez rechercher vos ressources, telles que les instances Amazon Elastic Compute Cloud, les flux Amazon Kinesis ou les tables Amazon DynamoDB en utilisant les métadonnées des ressources telles que les noms, les balises et les identifiants. L'explorateur de ressources est Régions AWS intégré à votre compte pour simplifier vos charges de travail interrégionales.

Resource Explorer fournit des réponses rapides à vos requêtes de recherche en utilisant des index créés et gérés par le Explorateur de ressources AWS service. Resource Explorer utilise diverses sources de données pour recueillir des informations sur les ressources de votreCompte AWS. Resource Explorer stocke ces informations dans les index que Resource Explorer peut rechercher.

Vous devez comprendre les concepts suivants pour administrer et configurer correctement Explorateur de ressources AWS pour vos utilisateurs.

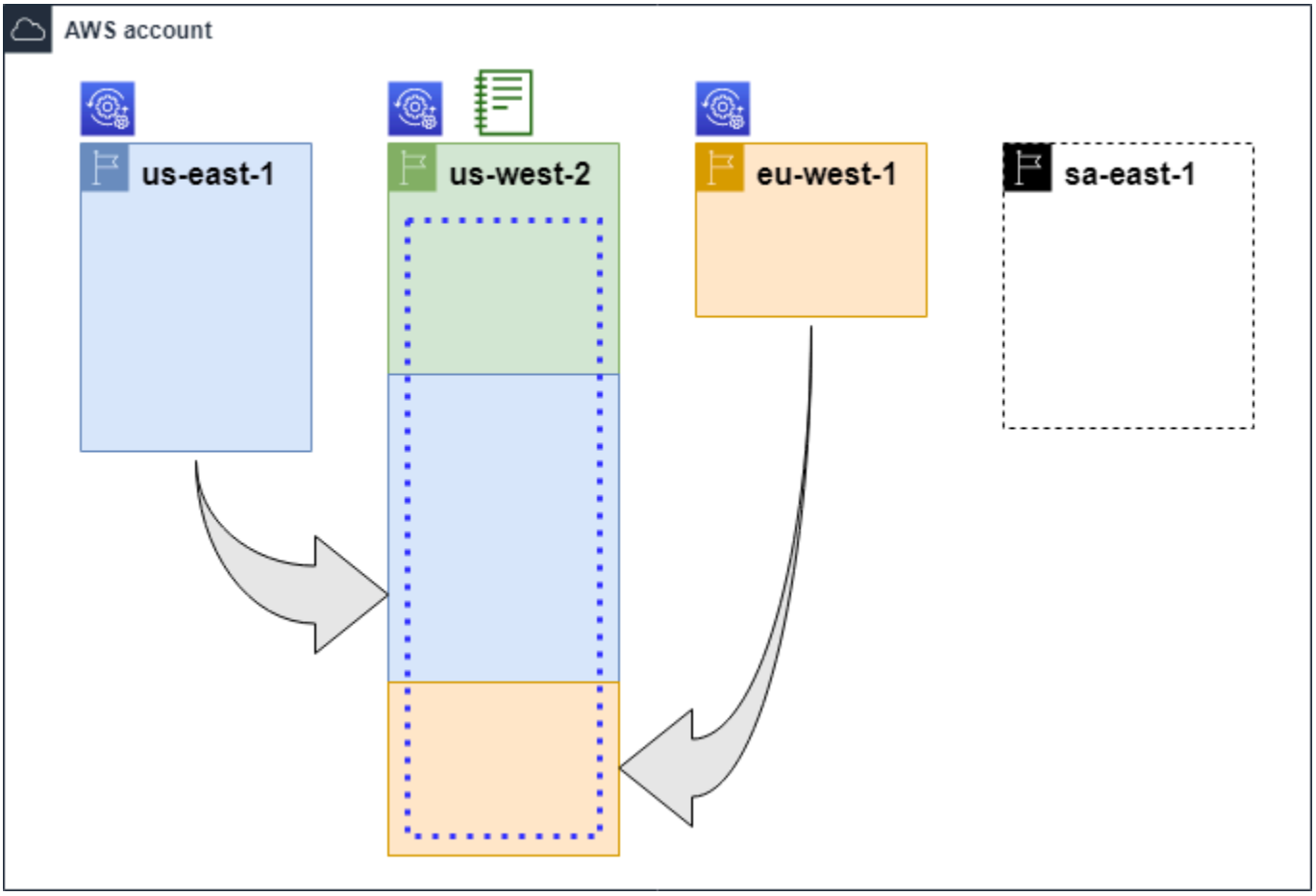
Concepts

- Administrateur de l'explorateur de ressources
- Utilisateur de l'explorateur de ressources
- Index
- Vue
- Ressource
- Recherche unifiée dans AWS Management Console
- Recherche multi-comptes

Le schéma suivant montre trois régions Régions AWS dans lesquelles l'administrateur a activé l'explorateur de ressources et une région que l'administrateur a choisi de ne pas activer. La région dans laquelle l'explorateur de ressources n'est pas activé ne possède pas d'index. Par conséquent, ses ressources ne peuvent pas être recherchées par des requêtes de l'explorateur de ressources.

Dans cet exemple de scénario, l'administrateur a choisi la région USA Ouest (Oregon) (`us-west-2`) pour contenir l'index agrégateur du compte. Toutes les régions que vous activez répliquent leurs index locaux dans la région à l'aide de l'index agrégateur.

La vue par défaut créée par Resource Explorer ne comporte aucun filtre. Par conséquent, les résultats d'une recherche avec cette vue peuvent inclure des ressources de tout type dans toutes les régions du compte où l'Explorateur de ressources est activé.



Légende	
	L'explorateur de ressources est alors activé Région AWS et les informations relatives aux ressources de la région sont stockées dans un index local de cette région. L'index local de chaque région est également répliqué (indiqué par les flèches) dans la région qui contient l'indice agrégateur.
	L'index qu'Région AWSil contient est configuré pour être l'index agrégateur du compte. Resource Explorer reproduit les informations sur les ressources collectées dans les index locaux de toutes les autres régions où Resource Explorer est activé dans l'index agrégateur de cette région. Les recherches effectuées dans cette région peuvent inclure les résultats de toutes les régions du compte.

La vue par défaut créée par Quick Setup inclut toutes les ressourcesRégions AWS.

Administrateur de l'explorateur de ressources

Un administrateur de Resource Explorer est un responsable AWS Identity and Access Management (IAM) autorisé à gérer Resource Explorer et ses paramètres au sein de l'. L'administrateur de Resource Explorer peut configurer les fonctionnalités suivantes :

- Activez l'explorateur de ressources pour chaque personne Régions AWS Compte AWS en créant des index dans ces régions. Cela permet à Resource Explorer de découvrir des ressources et de remplir l'index avec des informations sur ces ressources afin que les utilisateurs puissent rechercher des ressources dans cette région.
- Mettez à jour le type d'index en un Région AWS pour en faire l'index agrégateur correspondant à sonCompte AWS. L'index agrégateur de cette région reçoit des copies répliquées des informations sur les ressources provenant de toutes les autres régions du compte où Resource Explorer est activé.
- Créez des vues qui définissent le sous-ensemble d'informations indexées que les utilisateurs peuvent rechercher et découvrir dans Resource Explorer.
- Bien que cela ne fasse pas partie des actions de l'explorateur de ressources, l'administrateur de l'explorateur de ressources doit également être en mesure d'accorder des autorisations de recherche aux principaux utilisateurs du compte. L'administrateur peut accorder ces autorisations aux principaux en ajoutant les autorisations pertinentes aux politiques d'autorisation IAM existantes ou en utilisant la politique AWSgérée en lecture seule de Resource Explorer.

  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.

L'administrateur dispose généralement de toutes les autorisations de l'explorateur de ressources (`resource-explorer-2:*`) sur toutes les ressources de l'explorateur de ressources, y compris les index et les vues. Ces autorisations peuvent être accordées à l'aide de la politique AWS gérée d'accès complet de Resource Explorer.

Utilisateur de l'explorateur de ressources

Un utilisateur de Resource Explorer est un administrateur IAM autorisé à effectuer une ou plusieurs des tâches suivantes :

- Effectuez une recherche de ressources en utilisant une vue pour interroger l'explorateur de ressources. Un utilisateur de Resource Explorer souhaite découvrir et trouver AWS des ressources et utilise généralement la console Resource Explorer ou les `Search` opérations de l'explorateur de ressources fournies par AWS les SDK ou leAWS CLI.

  Un rôle ou un utilisateur peut utiliser IAM get permission pour effectuer une recherche à l'aide de l'une des deux méthodes suivantes :

  - Politique AWS gérée en lecture seule par l'explorateur de ressources pour le rôle, le groupe ou l'utilisateur IAM.
  - Une politique d'autorisation IAM avec une déclaration contenant les autorisations minimales suivantes pour le rôle, le groupe ou l'utilisateur IAM.

    ```
    {
        "Effect": "Allow",
        "Action": [
            "resource-explorer-2:Search",
            "resource-explorer-2:GetView",
        "Resource": "<ARN of the view>"
    }
    ```

- Bien que cela soit généralement considéré comme une tâche d'administrateur, vous pouvez déléguer à des utilisateurs de confiance la capacité de définir des vues et de créer des

vues. Pour ce faire, l'administrateur peut accorder l'autorisation d'appeler l'`resource-explorer-2:CreateView`opération dans le cadre d'une politique d'autorisation IAM attachée aux rôles, groupes ou utilisateurs concernés. Si la vue nécessite des autorisations spécifiques, des dispositions doivent être prises pour ajouter ou modifier les politiques IAM pour les utilisateurs concernés.

Pour plus d'informations sur la manière de rechercher des ressources à l'aide de l'Explorateur de ressources, consultezEn utilisantExplorateur de ressources AWSpour rechercher des ressources.

Index

Un index est la collection d'informations gérées par Resource Explorer sur toutes les AWS ressources d'une seule Région AWS de vos ressourcesCompte AWS. L'explorateur de ressources gère un index dans chaque région dans laquelle vous activez l'explorateur de ressources. Resource Explorer met automatiquement à jour l'index lorsque vous créez et supprimez des ressources dans votreCompte AWS. Dans le schéma précédent, les cases situées sous les Région AWS noms représentent les index de l'explorateur de ressources conservés dans chacun Région AWS d'eux. L'index d'une région est la source d'informations pour toutes les vues créées dans cette région. Les utilisateurs ne peuvent pas interroger directement l'index. Au lieu de cela, ils doivent toujours effectuer des requêtes à l'aide d'une vue.

Il existe deux types d'index :

Index local

Il existe un index local dans chaque index Région AWS dans lequel vous activez l'Explorateur de ressources. Un index local contient des informations uniquement sur les ressources d'une même région.

Indice agrégateur

L'administrateur de Resource Explorer peut également désigner l'index Région AWS d'un comme index agrégateur pour leCompte AWS. L'index agrégateur reçoit et stocke une copie de l'index pour toutes les autres régions dans lesquelles Resource Explorer est activé dans le compte. L'indice agrégateur reçoit et stocke également des informations sur les ressources de sa propre région. Dans le schéma précédent, la région `us-west-2` contient l'indice agrégateur du compte. La principale raison de désigner un index agrégateur pour le compte est de pouvoir créer des vues qui peuvent inclure des ressources provenant de toutes les régions du compte. Il ne peut y avoir qu'un seul indice agrégateur dans unCompte AWS.

Lorsque vous activez l'explorateur de ressources, vous pouvez spécifier lequel Région AWS doit contenir l'index de l'agrégateur. Vous pouvez également modifier ultérieurement l'indice Région AWS utilisé pour l'agrégateur. Pour plus d'informations sur la manière de promouvoir un indice local afin d'en faire l'indice agrégateur correspondantCompte AWS, consultezActivation de la recherche interrégionale en créant un index agrégateur.

Un index est une ressource portant un nom de ressource Amazon (ARN). Toutefois, vous ne pouvez utiliser cet ARN que dans les politiques d'autorisation pour accorder l'accès aux opérations qui interagissent directement avec l'index. Ces opérations vous permettent de créer des vues et de les définir comme vues par défaut dans une région, d'activer ou de désactiver l'explorateur de ressources dans une région et de créer un index agrégateur pour le compte. L'ARN d'un index ressemble à l'exemple suivant :

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111
```

Vue

Une vue est le mécanisme utilisé pour interroger les ressources répertoriées dans un index. La vue définit les informations de l'index qui sont visibles et disponibles à des fins de recherche et de découverte. Un utilisateur n'interroge jamais directement l'index de l'explorateur de ressources. Au lieu de cela, les requêtes doivent toujours passer par une vue qui permet au créateur de la vue de limiter les ressources que l'utilisateur peut voir dans les résultats de recherche.

Lorsque vous créez une vue, vous spécifiez des filtres qui limitent les ressources incluses dans les résultats de recherche. Par exemple, vous pouvez choisir d'inclure uniquement les ressources de quelques types de ressources spécifiques qui sont utilisées par les personnes auxquelles vous accordez l'accès à cette vue. Les résultats des requêtes effectuées par les utilisateurs avec une vue sont toujours automatiquement filtrés pour inclure uniquement les ressources qui répondent aux critères de la vue.

Pour accorder l'accès à une vue, vous pouvez attribuer des autorisations en utilisant l'une des méthodes suivantes.

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.

Accordez l'autorisation d'autoriser vos rôles, groupes ou utilisateurs à invoquer les `resource-explorer-2:Search` opérations `resource-explorer-2:GetView` et sur une vue identifiée par son nom de ressource Amazon (ARN). Vous pouvez également utiliser la politique AWS gérée en lecture seule de Resource Explorer pour tous les principaux qui ont besoin d'utiliser la vue pour effectuer des recherches. Vous pouvez créer plusieurs vues dotées de filtres et de portées différents et renvoyer ainsi différents sous-ensembles d'informations sur vos ressources. Vous pouvez ensuite accorder des autorisations pour chaque vue aux utilisateurs qui ont besoin de voir les informations incluses dans les résultats de cette vue.

Pour effectuer une recherche avec Resource Explorer, chaque utilisateur doit être autorisé à utiliser au moins une vue. Vous ne pouvez pas effectuer de recherche dans l'Explorateur de ressources sans utiliser une vue.

Les vues sont stockées par région. Une vue ne peut accéder qu'à l'index de l'explorateur de ressources qu'elle contientRégion AWS. Pour accéder aux résultats de recherche à l'échelle du compte, vous devez utiliser une vue dans la région qui contient l'index agrégateur du compte. L'option de configuration rapide crée une vue par défaut dans l'Région AWSindex de l'agrégateur et avec des filtres qui incluent toutes les ressources Régions AWS utilisées par le compte.

Pour plus d'informations sur la création de vues, consultezGestion des vues de l'explorateur de ressources pour fournir un accès à la recherche. Pour plus d'informations sur l'utilisation des vues dans une requête, consultezEn utilisantExplorateur de ressources AWSpour rechercher des ressources.

Chaque vue possède un nom de ressource Amazon (ARN) auquel vous pouvez faire référence dans les politiques d'autorisation pour accorder l'accès à des vues individuelles. Vous pouvez également transmettre l'ARN d'une vue en tant que paramètre à toute API ou AWS CLI opération interagissant avec une vue. L'ARN d'une vue ressemble à celui de l'exemple suivant.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> Chaque ARN de vue inclut un UUID AWS généré à la fin. Cela permet de garantir que les utilisateurs susceptibles d'avoir eu accès à des vues portant un nom spécifique qui a été supprimé ne puissent pas accéder automatiquement à une nouvelle vue créée avec le même nom.

Ressource

Une ressource est une entité avec AWS laquelle vous pouvez travailler. Les ressources sont créées au Services AWS fur et à mesure que vous utilisez les fonctionnalités du service. Les exemples incluent une instance Amazon EC2, un compartiment Amazon S3 ou une AWS CloudFormation pile. Certains types de ressources peuvent contenir des données client. Tous les types de ressources ont des attributs ou des métadonnées pour décrire la ressource, notamment un nom, une description et le nom de ressource Amazon (ARN) que vous utilisez pour référencer une ressource de manière unique. La plupart des types de ressources prennent également en charge les balises. Les balises sont des métadonnées personnalisées que vous pouvez associer à vos ressources à diverses fins, telles que la répartition des coûts dans votre facturation, l'autorisation de sécurité à l'aide d'un contrôle d'accès basé sur les attributs ou pour répondre à vos autres besoins de catégorisation.

L'objectif principal de Resource Explorer est de vous aider à trouver les ressources qui existent dans votreCompte AWS. Resource Explorer utilise diverses techniques pour découvrir toutes vos ressources et placer les informations les concernant dans un index. Vous pouvez ensuite interroger l'index par le biais des vues mises à votre disposition par votre administrateur.

> **Important**
>
> Resource Explorer exclut intentionnellement les types de ressources dont l'inclusion exposerait les données des clients. Les types de ressources suivants ne sont pas indexés par Resource Explorer et ne sont donc jamais renvoyés dans les résultats de recherche.
>
> - Objets Amazon S3 contenus dans un compartiment
> - Éléments de table Amazon DynamoDB
> - Valeurs des attributs DynamoDB

Recherche unifiée dans AWS Management Console

En haut de chaque AWS Management ConsoleService AWS, il y a une barre de recherche que vous pouvez utiliser pour rechercher une variété d'éléments AWS connexes. Vous pouvez rechercher des services et des fonctionnalités, et obtenir des liens directement vers la page correspondante dans la console de ce service. Vous pouvez également rechercher de la documentation et des articles de blog liés à votre terme de recherche.

Après avoir activé l'Explorateur de ressources et créé un index agrégateur et une vue par défaut, la recherche unifiée peut également inclure les ressources de votre compte dans les résultats de recherche. La recherche unifiée utilise automatiquement la vue par défaut dans le Région AWS qui contient l'index agrégateur du compte. Cela vous permet de rechercher une ressource depuis n'importe quelle page duAWS Management Console, sans avoir à ouvrir l'explorateur de ressources au préalable. Si vous ne promouvez pas d'index local comme index agrégateur du compte, ou si vous ne créez pas de vue par défaut dans la région de l'index agrégateur, la recherche unifiée n'inclut pas de ressources dans ses résultats de recherche. En outre, tout directeur effectuant une recherche doit être autorisé à utiliser la vue par défaut de la région qui contient l'index agrégateur, faute de quoi la recherche unifiée n'inclut pas de ressources dans ses résultats de recherche.

> **Important**
>
> La recherche unifiée insère automatiquement un opérateur de caractère générique (*) à la fin du premier mot clé de la chaîne. Cela signifie que les résultats de recherche unifiés incluent des ressources correspondant à n'importe quelle chaîne commençant par le mot clé spécifié.

La recherche effectuée par la zone de texte Requête sur la page de recherche de ressources de la console Resource Explorer n'ajoute pas automatiquement de caractère générique. Vous pouvez insérer un * manuellement après n'importe quel terme dans la chaîne de recherche.

Pour plus d'informations sur la recherche unifiée et son intégration à Resource Explorer, consultezUtilisation de la recherche unifiée dans AWS Management Console.

Recherche multi-comptes

Grâce à la recherche multi-comptes, vous pouvez rechercher et découvrir des ressources à l'AWS OrganizationsRégions AWSaide d'une seule recherche par mot clé.

Pour plus d'informations sur la recherche multi-comptes et sur la manière de l'activer pour Resource Explorer, consultezActivation de la recherche multi-comptes.

Conditions préalables à l'utilisation de l'explorateur de ressources

Avant de l'utiliser Explorateur de ressources AWS pour la première fois, effectuez les tâches suivantes selon vos besoins.

Tâches

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

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

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

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

Création d'un utilisateur doté d'un accès administratif

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

Sécurisez votre Utilisateur racine d'un compte AWS

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

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

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

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

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

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

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

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

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

Attribution d'un accès à d'autres utilisateurs

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

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

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

Configuration et configuration de l'explorateur de ressources

Avant de procéder à l'installation et à la configuration Explorateur de ressources AWS, assurez-vous que vous répondez aux prérequis. Ensuite, connectez-vous en tant que IAM rôle ou utilisateur disposant des autorisations requises pour effectuer les opérations de l'explorateur de ressources pour la procédure suivante.

Vous pouvez utiliser cette procédure d'installation et de configuration pour configurer Resource Explorer dans les comptes existants et dans tout nouveau compte ajouté à votre organisation.

Il existe deux méthodes pour configurer l'Explorateur de ressources :

- Configuration rapide
- Configuration avancée

Important

Si vous choisissez de configurer l'Explorateur de ressources à l'aide d'une option indiquant Régions AWS« toutes », il active uniquement celles Régions AWS qui existent et celles qui sont activées Compte AWS au moment où vous effectuez la procédure. L'explorateur de ressources ne s'active pas automatiquement dans Régions AWS les AWS applications ajoutées à l'avenir. Lorsque vous AWS introduisez une nouvelle région, vous pouvez choisir d'activer l'explorateur de ressources dans la région manuellement lorsqu'il apparaît sur la page Paramètres de la console de l'explorateur de ressources, ou en appelant l'CreateIndexopération.

Note

La configuration de l'explorateur de ressources peut également activer la possibilité de rechercher des ressources à l'aide de la barre de recherche unifiée sur le AWS Management Console. Pour que les utilisateurs puissent voir les ressources dans les résultats de recherche unifiés, vous devez configurer Resource Explorer avec un index agrégateur interrégional et une vue par défaut. Pour plus de détails, consultez les procédures suivantes. Vous devez également vous assurer que les utilisateurs qui effectuent des recherches sont autorisés à utiliser la vue par défaut dans le Région AWS contenant l'index de l'agrégateur. Pour de plus amples informations, veuillez consulter Utilisation de la recherche unifiée dans AWS Management Console.

Configuration de l'explorateur de ressources à l'aide de la configuration rapide

Si vous choisissez l'option de configuration rapide, Resource Explorer effectue les opérations suivantes :

- Crée un index Région AWS dans chaque élément de votre Compte AWS.
- Met à jour l'index dans la région que vous spécifiez comme indice agrégateur pour le compte.
- Crée une vue par défaut dans l'index de l'agrégateur Region. Cette vue ne comporte aucun filtre et renvoie donc toutes les ressources présentes dans l'index.

Autorisations minimales

Pour effectuer les étapes de la procédure suivante, vous devez disposer des autorisations suivantes :

- Action : `resource-explorer-2:*` — Ressource : aucune ressource spécifique (`*`)
- Action : `iam:CreateServiceLinkedRole` — Ressource : aucune ressource spécifique (`*`)

AWS Management Console

Pour configurer l'explorateur de ressources à l'aide de la configuration rapide

1. Ouvrez la Explorateur de ressources AWS console à l'adressehttps://console.aws.amazon.com/resource-explorer.
2. Choisissez Activer l'explorateur de ressources.
3. Sur la page Activer l'explorateur de ressources, sélectionnez Configuration rapide.
4. Choisissez celui dans lequel Région AWS vous souhaitez inclure l'index agrégateur. Vous devez sélectionner la région correspondant à l'emplacement géographique de vos utilisateurs.
5. Au bas de la page, choisissez Activer l'explorateur de ressources.
6. Sur la page Progression, vous pouvez suivre chacune d'elles au Région AWS fur et à mesure que Resource Explorer crée son index. La page affiche l'état de création de l'index agrégateur et de la création de la vue par défaut.

Une fois que toutes les étapes indiquent qu'elles ont été effectuées avec succès, vous et vos utilisateurs pouvez accéder à la page de recherche de ressources et commencer à rechercher des ressources.

> **Note**
>
> Les ressources balisées locales à l'index apparaissent dans les résultats de recherche en quelques minutes. Les ressources non balisées mettent généralement moins de deux heures à apparaître, mais cela peut prendre plus de temps en cas de forte demande. La réplication initiale vers un nouvel index agrégateur à partir de tous les index locaux existants peut également prendre jusqu'à une heure.

Prochaines étapes : avant que vos utilisateurs puissent effectuer des recherches avec la vue par défaut que vous venez de créer, vous devez leur accorder les autorisations nécessaires pour effectuer des recherches à l'aide de cette vue. Pour de plus amples informations, veuillez consulter Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

AWS CLI

La configuration de l'explorateur de ressources dans votre Compte AWS navigateur à l'aide de l'option de configuration avancée AWS CLI est, par définition, équivalente. Cela est dû au fait que les CLI opérations de l'explorateur de ressources n'exécutent aucune des étapes automatiquement à votre place, comme le fait la console de l'explorateur de ressources. Consultez l' AWS CLI onglet sur le Configuration de l'explorateur de ressources à l'aide de la configuration avancée pour voir quelles commandes sont équivalentes à l'utilisation de la console.

Configuration de l'explorateur de ressources à l'aide de la configuration avancée

Si vous choisissez l'option Configuration avancée, vous pouvez effectuer les opérations suivantes :

- Choisissez celui Régions AWS dans lequel vous souhaitez activer l'Explorateur de ressources.
- Choisissez si vous souhaitez configurer une région avec un index agrégateur. Si c'est le cas, vous spécifiez Région AWS le dans lequel le placer. Cet index vous permet de créer des vues qui peuvent inclure des ressources de toutes les régions du compte. Pour plus d'informations, voir Activation de la recherche interrégionale en créant un index agrégateur.
- Choisissez si vous souhaitez créer une vue par défaut. Cette vue permet de rechercher automatiquement n'importe quelle AWS ressource dans les régions dans lesquelles vous activez l'Explorateur de ressources. Vous devez vous assurer que tous les principaux qui doivent utiliser la vue par défaut pour effectuer une recherche dans l'Explorateur de ressources disposent des autorisations d'accès à cette vue. Pour de plus amples informations, veuillez consulter Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

> **Note**
>
> Vous pouvez configurer l'explorateur de ressources pour inclure vos ressources dans les résultats de recherche fournis par la fonction de recherche unifiée du AWS Management Console. Pour activer cette fonctionnalité, vous devez configurer Resource Explorer avec un

index agrégateur et une vue par défaut dans laquelle tous les rôles et utilisateurs peuvent effectuer des recherches. L'option de configuration rapide crée à la fois l'index de l'agrégateur et la vue par défaut. C'est pourquoi nous vous recommandons d'activer l'explorateur de ressources.

Autorisations minimales

Pour effectuer les étapes de la procédure suivante, vous devez disposer des autorisations suivantes :

- Action : `resource-explorer-2:*` — Ressource : aucune ressource spécifique (`*`)
- Action : `iam:CreateServiceLinkedRole` — Ressource : aucune ressource spécifique (`*`)

AWS Management Console

Pour activer l'explorateur de ressources à l'aide de la configuration avancée

1. Ouvrez la Explorateur de ressources AWS console à l'adressehttps://console.aws.amazon.com/resource-explorer.
2. Choisissez Activer l'explorateur de ressources.
3. Sur la page Activer l'explorateur de ressources, choisissez Configuration avancée.
4. Dans la Régions AWSzone, sous Régions, indiquez si vous souhaitez activer l'explorateur de ressources dans toutes les Régions AWS régions ou uniquement dans des régions spécifiques.

   Si vous choisissez Activer l'explorateur de ressources uniquement dans les zones spécifiées Régions AWS dans ce compte, sélectionnez chaque région dont vous souhaitez inclure les ressources dans les résultats de recherche.
5. Pour l'index agrégateur, indiquez si vous souhaitez créer un index agrégateur. Si vous choisissez de créer un index agrégateur, tous les autres Régions AWS répliquent leurs index dans cette région. Cela permet aux utilisateurs de rechercher des ressources dans toutes les régions sélectionnées dans le Compte AWS. Choisissez celui Région AWS qui contient l'index agrégateur. Nous vous recommandons de spécifier la région dans laquelle vos utilisateurs passent le plus clair de leur temps, ou du moins dans laquelle vous pensez qu'ils effectueront la plupart de leurs recherches de ressources.
6. Dans la zone Affichage par défaut, sous Création de vue, indiquez si vous souhaitez créer un affichage par défaut. Cette option n'est disponible que si vous avez choisi de créer un

index agrégateur. Si vous choisissez de créer une vue par défaut, Resource Explorer place cette vue au même endroit Région AWS que l'index de l'agrégateur. Cela permet à la vue par défaut d'inclure les résultats de tous Régions AWS ceux dans lesquels vous avez enregistré Resource Explorer. Chaque fois qu'un utilisateur effectue une recherche dans une région avec une vue par défaut et ne spécifie pas explicitement de vue, la recherche utilise la vue par défaut pour cette région.

> **Note**
>
> Avant que vos utilisateurs puissent effectuer une recherche avec une vue, vous devez leur accorder l'autorisation d'utiliser cette vue. Pour de plus amples informations, veuillez consulter Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

7. Choisissez Activer l'explorateur de ressources.

> **Note**
>
> Les ressources balisées locales à l'index apparaissent dans les résultats de recherche en quelques minutes. Les ressources non balisées mettent généralement moins de deux heures à apparaître, mais cela peut prendre plus de temps en cas de forte demande. La réplication initiale vers un nouvel index agrégateur à partir de tous les index locaux existants peut également prendre jusqu'à une heure.

AWS CLI

Pour configurer l'explorateur de ressources à l'aide de la configuration avancée

La console Resource Explorer exécute de nombreux appels d'APIopérations en votre nom en fonction des choix que vous faites. Les exemples de AWS CLI commandes suivants montrent comment exécuter les mêmes procédures de base en dehors de la console à l'aide du AWS CLI.

Example Étape 1 : Activez l'explorateur de ressources en créant des index dans le champ souhaité Régions AWS

Exécutez la commande suivante dans chacune des commandes Région AWS dans lesquelles vous souhaitez activer Resource Explorer. L'exemple de commande suivant active l'Explorateur de ressources dans le Région AWS paramètre par défaut pour AWS CLI.

```
$ aws resource-explorer-2 create-index
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example Étape 2 : Mettez à jour l'indice en un Région AWS pour qu'il devienne l'indice agrégateur du compte

Exécutez la commande suivante Région AWS dans laquelle vous souhaitez que Resource Explorer mette à jour l'index local en fonction de l'index agrégateur du compte. L'exemple de commande suivant met à jour l'index de l'agrégateur dans l'est des États-Unis (Virginie du Nord) (`us-east-1`).

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
    "Type": "AGGREGATOR"
}
```

Example Étape 3 : créer une vue dans le Région AWS contenant l'index de l'agrégateur

Exécutez la commande suivante dans le fichier Région AWS dans lequel vous avez créé l'index de l'agrégateur. L'exemple de commande suivant crée une vue identique à celle créée par le processus de configuration de la console Resource Explorer. Cette nouvelle vue inclut les balises associées à la ressource dans le cadre des informations indexées et permet de rechercher des ressources par clé ou valeur de balise.

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
```

```
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example Étape 4 : Définissez votre nouvelle vue comme vue par défaut pour son Région AWS

L'exemple suivant définit la vue que vous avez créée à l'étape précédente comme vue par défaut pour la région. Vous devez exécuter la commande suivante dans la même fenêtre que celle Région AWS dans laquelle vous avez créé la vue par défaut.

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

Avant que vos utilisateurs puissent effectuer une recherche avec une vue, vous devez leur accorder l'autorisation d'utiliser cette vue. Pour de plus amples informations, veuillez consulter Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

Après avoir exécuté ces commandes, Resource Explorer s'exécute dans les régions spécifiées dans votre Compte AWS. Resource Explorer crée et gère un index dans chaque région avec des détails sur les ressources qui s'y trouvent. Resource Explorer réplique chacun des index de région individuels sur l'index agrégateur de la région spécifiée. Cette région contient également une vue qui permet à n'importe quel IAM rôle ou utilisateur du compte de rechercher des ressources dans toutes les régions indexées.

> **Note**
>
> Les ressources balisées locales à l'index apparaissent dans les résultats de recherche en quelques minutes. Les ressources non balisées mettent généralement moins de deux heures à apparaître, mais cela peut prendre plus de temps en cas de forte demande. La réplication initiale vers un nouvel index agrégateur à partir de tous les index locaux existants peut également prendre jusqu'à une heure.

Identifiez ceux sur Régions AWS lesquels l'explorateur de ressources est activé

Vous pouvez identifier ceux qui Régions AWS sont Explorateur de ressources AWS activés en vérifiant si la région contient un index pour Resource Explorer. Pour voir quelles régions disposent d'un index, suivez les procédures décrites sur cette page.

> **Important**
>
> Les utilisateurs peuvent rechercher des ressources uniquement dans les régions où l'Explorateur de ressources est activé. Vous pouvez également créer un index agrégateur dans une région pour faciliter la recherche de ressources dans toutes vos régions. L'explorateur de ressources réplique les informations sur les ressources dans la région à l'aide de l'index agrégateur de toutes les autres régions contenant un index d'explorateur de ressources. Les utilisateurs ne peuvent pas utiliser l'explorateur de ressources pour découvrir des ressources dans des régions dépourvues d'index.

Vérifier le statut de l'explorateur de ressources dans une région

Vous pouvez vérifier quelles régions ont des index pour Resource Explorer en utilisant le AWS Management Console, en utilisant les commandes dans le AWS Command Line Interface (AWS CLI) ou en utilisant les API opérations dans un AWS SDK.

AWS Management Console

Pour vérifier quelles régions disposent d'index pour Resource Explorer

1. Ouvrez la page Paramètres dans la console Resource Explorer.
2. La liste de la section Indexes inclut uniquement les régions contenant un index Resource Explorer. La valeur de la colonne Type indique si l'index est un index local pour sa région ou un index agrégateur pour le Compte AWS.
3. Pour voir quelles régions ne contiennent pas d'explorateur de ressources, choisissez Créer des index. Si aucune région n'est présente, elle ne contient pas l'explorateur de ressources.

AWS CLI

Pour vérifier quelles régions disposent d'index pour Resource Explorer

Exécutez la commande suivante pour voir lesquels Régions AWS contiennent des index pour Resource Explorer.

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

Activer l'explorateur de ressources Région AWS pour indexer vos ressources

Lorsque vous avez initialement activé Explorateur de ressources AWS votre Compte AWS, vous avez créé des index pour le service dans un ou plusieurs Régions AWS. Si vous avez utilisé l'option de configuration rapide, Resource Explorer a automatiquement créé des index dans tous Régions AWS ceux qui sont activés dans votre Compte AWS. Le service Resource Explorer a également promu l'index de la région spécifiée en tant qu'index agrégateur du compte. Si vous avez utilisé l'option de configuration avancée, vous avez spécifié les régions dans lesquelles créer les index.

Rubriques

- Création d'un index d'explorateur de ressources dans une région
- Considérations relatives aux AWS régions optionnelles

Lorsque vous activez l'explorateur de ressources dans un Région AWS, le service exécute les actions suivantes :

- Lorsque vous démarrez Resource Explorer dans la première région d'un Compte AWS, Resource Explorer crée un rôle lié à un service dans le compte nommé. `AWSServiceRoleForResourceExplorer` Ce rôle autorise Resource Explorer à découvrir et à indexer les ressources de votre compte à l'aide de services tels que AWS CloudTrail le service de balisage. La création du rôle lié au service n'a lieu que lorsque vous enregistrez le premier rôle Région AWS dans le compte. Resource Explorer utilise le même rôle lié à un service pour toutes les régions supplémentaires que vous ajouterez ultérieurement.
- L'explorateur de ressources crée un index dans la région spécifiée pour stocker les détails des ressources de cette région.
- L'explorateur de ressources commence à découvrir les ressources de la région spécifiée et ajoute les informations qu'il trouve à leur sujet à l'index de cette région.
- Si votre compte contient déjà un index agrégateur dans une autre région, Resource Explorer commence à répliquer les informations de l'index de la nouvelle région vers l'index agrégateur afin de faciliter la recherche entre régions.

Lorsque ces étapes sont terminées, les informations relatives à vos ressources peuvent être découvertes par les utilisateurs. Ils peuvent effectuer une recherche en utilisant l'une des vues définies dans la même région ou dans la région qui contient l'index agrégateur.

Création d'un index d'explorateur de ressources dans une région

Vous pouvez créer un index Resource Explorer dans un index supplémentaire en Région AWS utilisant le AWS Management Console, en utilisant des commandes dans le AWS Command Line Interface (AWS CLI) ou en utilisant API des opérations dans un AWS SDK. Vous ne pouvez créer qu'un seul index par région.

Autorisations minimales

Pour effectuer les étapes de la procédure suivante, vous devez disposer des autorisations suivantes :

- Action : `resource-explorer-2:*` — Ressource : aucune ressource spécifique (`*`)
- Action : `iam:CreateServiceLinkedRole` — Ressource : aucune ressource spécifique (`*`)

AWS Management Console

Pour créer un index Resource Explorer dans un Région AWS

1. Sur la page des paramètres de l'explorateur de ressources.
2. Dans la section Index, sélectionnez Créer des index.
3. Sur la page Créer des index, cochez les cases à côté de celles Régions AWS dans lesquelles vous souhaitez créer un index pour faciliter la recherche dans les ressources de cette région. Les cases à cocher non disponibles indiquent les régions qui contiennent déjà un index Resource Explorer.
4. (Facultatif) Dans la section Balises, vous pouvez spécifier les paires clé/valeur de balise pour l'index.
5. Choisissez Créer des index.

   L'explorateur de ressources affiche une bannière verte en haut de la page pour indiquer le succès, ou une bannière rouge en cas d'erreur lors de la création d'un index dans une ou plusieurs des régions sélectionnées.

> **Note**
>
> Les ressources balisées locales à l'index apparaissent dans les résultats de recherche en quelques minutes. Les ressources non balisées mettent généralement moins de deux heures à apparaître, mais cela peut prendre plus de temps en cas de forte demande. La réplication initiale vers un nouvel index agrégateur à partir de tous les index locaux existants peut également prendre jusqu'à une heure.

Étape suivante — Si vous avez déjà créé un index agrégateur, les nouvelles régions commencent automatiquement à répliquer leurs informations d'index dans l'index agrégateur. Si c'est là que vos utilisateurs effectuent toutes leurs recherches, les ressources de la nouvelle région apparaissent dans les résultats de recherche et vous avez terminé.

Toutefois, si vous souhaitez que les utilisateurs puissent rechercher des ressources uniquement dans la région nouvellement indexée, vous devez également créer une vue pour les utilisateurs de cette région et autoriser vos utilisateurs à accéder à cette vue. Pour obtenir des instructions sur la création d'une vue, consultezGestion des vues de l'explorateur de ressources pour fournir un accès à la recherche.

AWS CLI

Pour créer un index Resource Explorer dans un Région AWS

Exécutez la commande suivante pour chaque Région AWS élément dans lequel vous souhaitez créer un index afin de faciliter la recherche dans les ressources de cette région. L'exemple de commande suivant enregistre Resource Explorer dans l'est des États-Unis (Virginie du Nord) (`us-east-1`).

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

Répétez cette commande pour chaque région dans laquelle vous souhaitez activer l'explorateur de ressources, en remplaçant le code de région approprié par le `--region` paramètre.

Comme Resource Explorer effectue une partie de la création d'index sous forme de tâches asynchrones en arrière-plan, la réponse peut êtreCREATING, ce qui indique que les processus en arrière-plan ne sont pas encore terminés.

> **Note**
>
> Les ressources balisées locales à l'index apparaissent dans les résultats de recherche en quelques minutes. Les ressources non balisées mettent généralement moins de deux heures à apparaître, mais cela peut prendre plus de temps en cas de forte demande. La réplication initiale vers un nouvel index agrégateur à partir de tous les index locaux existants peut également prendre jusqu'à une heure.

Vous pouvez vérifier l'achèvement final en exécutant la commande suivante et en vérifiant l'ACTIVEétat.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

Étape suivante — Si vous avez déjà créé un index agrégateur, les nouvelles régions commencent automatiquement à répliquer leurs informations d'index dans l'index agrégateur. Si c'est là que vos utilisateurs effectuent toutes leurs recherches, les ressources de la nouvelle région apparaissent dans les résultats de recherche et vous avez terminé.

Toutefois, si vous souhaitez que les utilisateurs puissent rechercher des ressources uniquement dans la région nouvellement indexée, vous devez également créer une vue pour les utilisateurs de cette région et autoriser vos utilisateurs à accéder à cette vue. Pour obtenir des instructions sur

la création d'une vue, consultezGestion des vues de l'explorateur de ressources pour fournir un accès à la recherche.

Considérations relatives aux AWS régions optionnelles

Les régions optionnelles ont des exigences de sécurité plus élevées que les régions commerciales en ce qui concerne le partage de IAM données par le biais de comptes dans les régions optionnelles. Toutes les données gérées par le biais du IAM service sont considérées comme des données d'identité.

Vous pouvez activer les régions optionnelles à l'aide de la Explorateur de ressources AWS console. Pour plus d'informations, voir Activer l'explorateur Région AWS de ressources dans un pour indexer vos ressources.

Comportements d'exclusion

Tenez compte des comportements suivants avant de vous désinscrire d'une région optionnelle :

> **Important**
>
> Avant de vous désinscrire d'une région dotée d'un index agrégateur, nous vous suggérons de supprimer l'index agrégateur ou de le rétrograder au rang d'index local. Resource Explorer prend en charge un index agrégateur pour toutes les régions de la partition.

- Votre index n'est pas supprimé, il est simplement désactivé. Si vous choisissez de vous réinscrire ultérieurement, vos paramètres seront rétablis.
- IAMdésactive IAM l'accès aux ressources de la région.
- L'explorateur de ressources désactive l'index pour la région désactivée et arrête l'ingestion de données. L'index des régions `ListIndexes` API ne sera plus affiché.
- Si votre index agrégateur se trouve dans une autre région, Resource Explorer arrête la réplication des données depuis la région désactivée et nettoie les données dans les 24 heures.
- Si vous vous désabonnez de votre région d'index agrégateur, vous devrez vous réinscrire pour supprimer ou rétrograder l'indice.
- Si vous vous inscrivez à nouveau à la région, Resource Explorer réactive l'index et commence à ingérer des données.

- Toute modification du statut d'une région optionnelle prend environ 24 heures pour entrer en vigueur.

Activation de la recherche interrégionale en créant un index agrégateur

Lorsque la recherche interrégionale est activée, vous pouvez rechercher des ressources dans toutes les régions de votre Compte AWS.

Rubriques

À propos de l'indice agrégateur

Explorateur de ressources AWS stocke les informations collectées sur les ressources dans un Région AWS index local que Resource Explorer crée et gère dans cette région. Supposons, par exemple, que vous disposiez d'une EC2 instance Amazon dans la région de l'ouest des États-Unis (Oregon). L'explorateur de ressources stocke les informations relatives à cette ressource dans l'index local de la région USA Ouest (Oregon).

Pour faciliter la recherche de ressources Régions AWS dans l'ensemble de votre compte, vous pouvez convertir l'index local d'une région en index agrégateur pour votre compte.

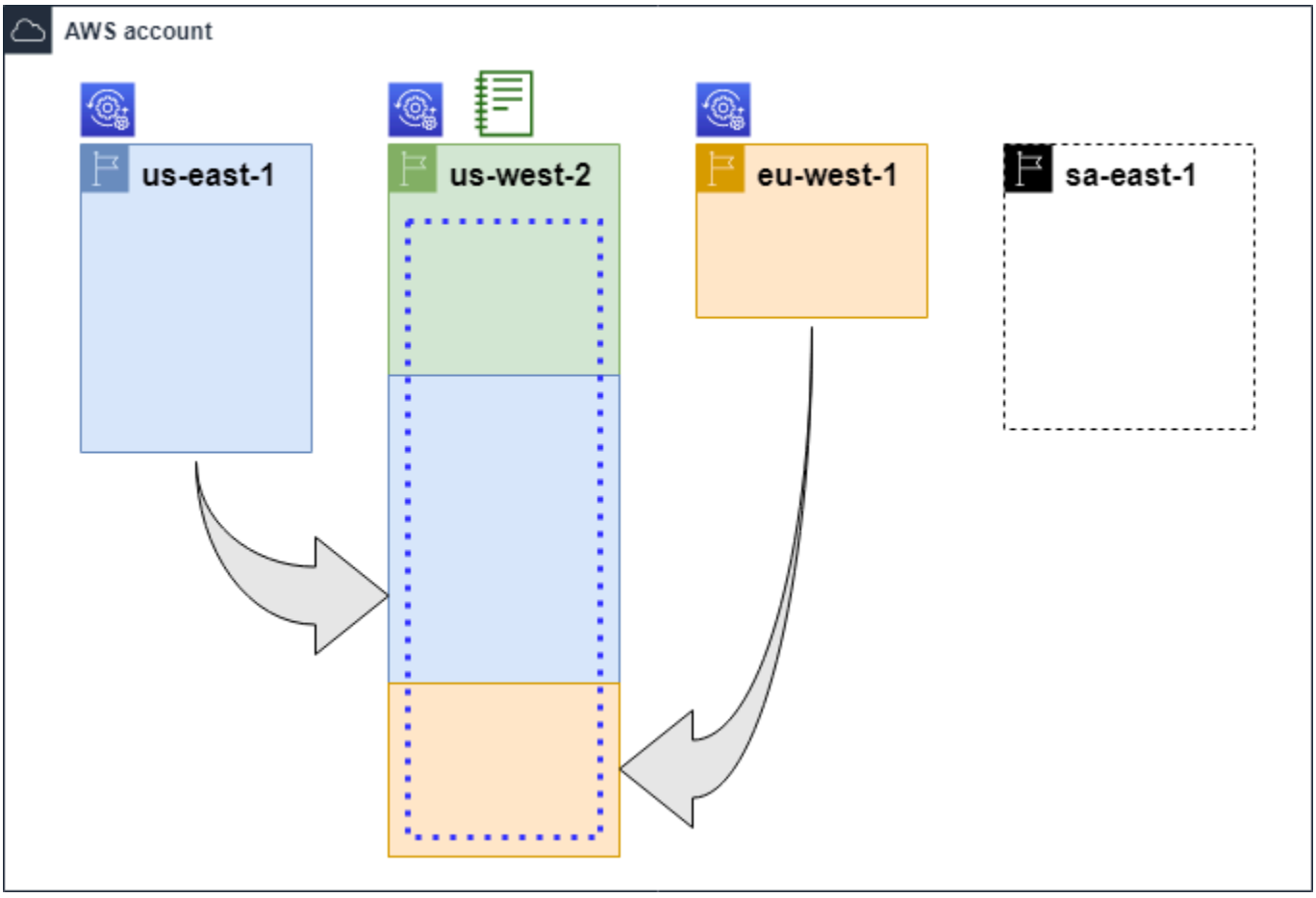
L'index agrégateur contient une copie répliquée de l'index local dans toutes les autres régions où vous avez activé l'explorateur de ressources. Cela vous permet de créer des vues dans la région qui contient l'index agrégateur dont les résultats peuvent inclure les ressources de tous Régions AWS les utilisateurs du compte.

Le schéma suivant montre un exemple du fonctionnement de l'indice agrégateur. Dans cet exemple Compte AWS, l'administrateur effectue les opérations suivantes :

- Active l'explorateur de ressources en trois Régions AWS (`us-east-1`us-west-2, eteu-west-1) en créant des index dans ces régions. Chaque région contient son propre index local.
- Choisit de ne pas créer d'index dans la `sa-east-1` région. Les utilisateurs ne peuvent pas effectuer de recherches dans `sa-east-1` cette région et aucune ressource de cette région n'apparaît dans les résultats de recherche.

- Crée l'index agrégateur pour le compte dans la `us-west-2` région. Cela oblige Resource Explorer à répliquer les informations des index locaux de toutes les autres régions où Resource Explorer est activé dans l'index agrégateur. Cela permet aux recherches effectuées `us-west-2` d'inclure les ressources des trois régions dans lesquelles l'explorateur de ressources est activé.

Cette configuration signifie qu'un utilisateur peut effectuer des recherches interrégionales uniquement dans`us-west-2`, qui contient l'index de l'agrégateur. Seules les vues de cette région peuvent renvoyer les résultats de toutes les régions du compte.



Légende	
	L'explorateur de ressources est activé dans ce Région AWS cas, et ses ressources sont cataloguées dans un index dans cette région. L'indice de cette région est également reproduit (indiqué par les flèches) sur Région AWS celui qui contient l'indice agrégateur.

	Il Région AWS contient l'indice de l'agrégateur. Resource Explorer reproduit les informations sur les ressources collectées dans toutes les autres régions Régions AWS dans cette région.
	La vue par défaut créée par Quick Setup inclut toutes les ressources Régions AWS.

Promouvoir un indice local en tant qu'indice agrégateur pour le compte

Vous avez la possibilité de créer un index agrégateur en un seulRégion AWS lors de la première configurationExplorateur de ressources AWS. Pour plus d'informations, consultez Configuration et configuration de l'explorateur de ressources. Cette procédure consiste à promouvoir l'un des index locaux en tant qu'index agrégateur pour le compte si vous ne l'avez pas fait lors de la configuration initiale.

⚠ Important

- Vous ne pouvez avoir qu'un seul index d'agrégation dans unCompte AWS. Si le compte possède déjà un index agrégateur, vous devez d'abord le rétrograder dans un index local ou le supprimer.
- Après avoir supprimé ou modifié la région qui contient l'index agrégateur, vous devez attendre 24 heures avant de pouvoir promouvoir un autre index en tant qu'index agrégateur.

AWS Management Console

Pour promouvoir un indice local en tant qu'indice agrégateur pour le compte

1. Ouvrez la page Paramètres de l'explorateur de ressources.
2. Dans la section Index, cochez la case à côté de l'index que vous souhaitez promouvoir, puis choisissez Modifier le type d'index.
3. Dans la boîte de dialogue Modifier le type d'index pour < Nom de la région >, choisissez l'index agrégateur, puis choisissez Enregistrer les modifications.

AWS CLI

Pour promouvoir un indice local en tant qu'indice agrégateur pour le compte

L'exemple de commande suivant met à jour l'indexRégion AWS du typeLOCAL au type spécifiéAGGREGATOR. Vous devez appeler l'opération à partir deRégion AWS laquelle vous souhaitez contenir l'index de l'agrégateur.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"AGGREGATOR"
}
```

L'opération fonctionne de manière asynchrone et commence parState set toUPDATING. Pour vérifier si l'opération est terminée, vous pouvez exécuter la commande suivante et rechercher la valeurACTIVE dans le champ deState réponse. Vous devez exécuter cette commande dans la région qui contient l'index que vous souhaitez vérifier.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

Rétrogradation de l'index agrégateur en index local

Vous pouvez rétrograder un index agrégateur en index local, par exemple lorsque vous souhaitez déplacer l'index agrégateur vers un autre. Région AWS

Lorsque vous rétrogradez un index agrégateur en index local, Resource Explorer arrête de répliquer les index à partir d'un autre index. Régions AWS Il lance également une tâche d'arrière-plan asynchrone pour supprimer toutes les informations répliquées provenant d'autres régions. Jusqu'à ce que cette tâche asynchrone soit terminée, certains résultats interrégionaux peuvent continuer à apparaître dans les résultats de recherche.

Remarques

- Après avoir rétrogradé un indice agrégateur, vous devez attendre 24 heures avant de pouvoir promouvoir le même indice ou l'indice d'une autre région en tant que nouvel indice agrégateur pour le compte.
- Après la rétrogradation d'un index agrégateur, il peut s'écouler jusqu'à 36 heures pour que les processus en arrière-plan soient terminés et que toutes les informations sur les ressources provenant d'autres régions disparaissent des résultats des recherches effectuées dans cette région.
- Si vous rétrogradez un compte membre dans une vue globale de l'organisation, le membre peut être retiré de la recherche multi-comptes.

Vous pouvez vérifier l'état de la tâche en arrière-plan en consultant la liste des index sur la page Paramètres ou en utilisant l'GetIndexopération. Lorsque les tâches asynchrones sont terminées, le `Status` champ de l'index passe de à`UPDATING`. `ACTIVE` À ce stade, seuls les résultats de la région locale apparaissent dans les résultats de la requête.

AWS Management Console

Pour rétrograder un index agrégateur en index local

1. Ouvrez la page des paramètres de l'explorateur de ressources.
2. Dans la section Index, cochez la case à côté de la région contenant l'index agrégateur que vous souhaitez rétrograder en index local, puis choisissez Modifier le type d'index.

3. Dans la boîte de dialogue Modifier le type d'index pour < Nom de région >, choisissez Index local, puis Enregistrer les modifications.

AWS CLI

Pour rétrograder un index agrégateur en index local

L'exemple suivant rétrograde l'index agrégateur spécifié en index local. Vous devez appeler l'opération dans le fichier Région AWS qui contient actuellement l'index agrégateur.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
}
```

L'opération fonctionne de manière asynchrone et commence par `State` set to. `UPDATING` Pour vérifier si l'opération est terminée, vous pouvez exécuter la commande suivante et rechercher la valeur `ACTIVE` dans le champ de `State` réponse. Vous devez exécuter cette commande dans la région qui contient l'index que vous souhaitez vérifier.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
```

```
    "Type": "LOCAL"
}
```

Activation de la recherche multi-comptes

Grâce à la recherche multicompte, vous pouvez rechercher des ressources sur des comptes dotés d'index actifs dans votre unité organisationnelle (UO) AWS Organizations ou dans votre unité organisationnelle (UO).

Rubriques

Prérequis

Pour activer la recherche multi-comptes pour votre organisation, procédez comme suit :

- Pour les régions éligibles, vérifiez que votre compte de gestion est également activé lorsque vous activez la recherche multi-comptes.
- Créez un utilisateur administratif.
- Créez un rôle lié à un service dans le compte administrateur avec. `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`
- Activez un accès sécurisé dans AWS Organizations. Cela permet une intégration complète avec Resource Explorer pour répertorier les ressources de tous les comptes de votre organisation.
- Désignez un administrateur délégué (recommandé). Pour plus d'informations, consultez la section Administrateur délégué pour les AWS services compatibles avec les Organizations dans le Guide de AWS Organizations l'utilisateur.
  - Resource Explorer ne prend en charge qu'un seul administrateur délégué qui exécute des actions similaires au compte de gestion.
  - La suppression ou la modification de l'administrateur délégué de votre organisation entraîne la suppression de toutes les vues multi-comptes créées dans son compte.

Activer la recherche multi-comptes

Pour rechercher et découvrir des ressources dans les comptes de votre organisation, vous devez suivre les étapes suivantes :

1. Activez Explorateur de ressources AWS dans un ou plusieurs comptes de votre AWS Organizations.
2. Enregistrez une région pour contenir l'index agrégateur.
3. Choisissez une région dans laquelle vous souhaitez créer un index agrégateur. Cette région doit être cohérente dans l'ensemble de votre AWS Organizations.
4. Créez une vue de l'explorateur de ressources limitée à votre unité organisationnelle AWS Organizations ou à votre unité organisationnelle. Créez cette vue dans la région de l'agrégateur à partir de l'étape précédente.
5. Partagez la vue avec les comptes de votre organisation.

Configuration rapide pour plusieurs comptes

Activez l'explorateur de ressources sur plusieurs comptes de votre organisation grâce à la configuration rapide.

> **Note**
>
> Ce processus ne déploie aucune ressource dans le compte de gestion. Si vous utilisez le compte de gestion et que vous souhaitez y ajouter des index, vous devez les ajouter manuellement dans le flux d'intégration de Resource Explorer.

1. Accédez à Quick Setup for Resource Explorer dans la console Systems Manager.
2. Choisissez la région de votre index agrégateur. Cela vous permet de rechercher des ressources situées dans toutes les régions dans les comptes cibles sélectionnés. Si l'un des comptes cibles sélectionnés possède déjà un index agrégateur configuré dans une autre région, l'index agrégateur existant sera automatiquement remplacé par cette nouvelle région.
3. Choisissez les cibles de votre compte. Vous pouvez activer l'Explorateur de ressources pour l'ensemble de votre organisation ou pour des unités organisationnelles spécifiques (OUs).

> **Note**
>
> Vous pouvez déployer jusqu'à 50 000 AWS CloudFormation piles à la fois. Si vous avez une grande organisation qui couvre plusieurs régions, vous devez effectuer le déploiement au niveau de l'unité d'organisation par petits lots.

4. Lisez le résumé des remerciements avant de choisir Créer.

Effet des actions du compte sur la recherche multi-comptes de Resource Explorer

> **Note**
>
> Il faut jusqu'à 24 heures pour supprimer des comptes et des ressources des résultats de recherche multi-comptes.

Les actions de compte ont les effets suivants sur la recherche Explorateur de ressources AWS multi-comptes.

Explorateur de ressources désactivé

Lorsque vous désactivez l'Explorateur de ressources pour un compte, il est désactivé uniquement pour ce compte dans le Région AWS compte sélectionné lorsque vous le désactivez.

Vous devez désactiver l'explorateur de ressources séparément dans chaque région où il est activé.

Après 24 heures, les ressources de ce compte n'apparaîtront pas dans les résultats de recherche.

Les autres données et paramètres de Resource Explorer ne sont pas supprimés.

Le compte de membre est supprimé d'une organisation

Lorsqu'un compte membre est supprimé d'une organisation, le compte administrateur Resource Explorer perd l'autorisation d'afficher les ressources du compte membre.

Si le compte supprimé est un compte administrateur ou administrateur délégué, toutes les vues multi-comptes précédemment créées par ces comptes seront également supprimées.

Resource Explorer continue de fonctionner dans les deux comptes.

Les résultats de recherche de ressources n'incluent plus les ressources de ce compte.

Le compte est suspendu

Lorsqu'un compte est suspendu AWS, il perd l'autorisation d'afficher les ressources dans l'Explorateur de ressources. Le compte administrateur d'un compte suspendu peut consulter les ressources existantes.

Pour un compte d'organisation, le statut du compte membre peut également passer à Compte suspendu. Cela se produit si le compte est suspendu au moment où le compte administrateur tente de l'activer. Le compte administrateur d'un compte suspendu ne peut pas consulter les ressources de ce compte.

Dans le cas contraire, le statut suspendu n'affecte pas le statut du compte du membre.

Après 90 jours, le compte est soit désactivé, soit réactivé. Lorsque le compte est réactivé, ses autorisations d'explorateur de ressources sont restaurées. Si le statut du compte membre est Compte suspendu, le compte administrateur doit activer le compte manuellement.

Le compte est fermé

Lorsqu'un AWS compte est fermé, Resource Explorer répond à la fermeture comme suit :

- Resource Explorer conserve les ressources du compte pendant 90 jours à compter de la date effective de fermeture du compte. À la fin de la période de 90 jours, Resource Explorer supprime définitivement toutes les ressources du compte.
- Pour conserver les ressources pendant plus de 90 jours, vous pouvez utiliser une action personnalisée avec une EventBridge règle pour stocker les ressources dans un compartiment Amazon S3. Tant que Resource Explorer conserve les ressources, lorsque vous rouvrez le compte fermé, Resource Explorer restaure les ressources du compte.
- Si le compte est un compte administrateur Resource Explorer, il est supprimé en tant qu'administrateur et tous les comptes des membres sont supprimés. S'il s'agit d'un compte membre, il est dissocié et supprimé en tant que membre du compte administrateur de Resource Explorer.
- Pour plus d'informations, consultez Clôture d'un compte.

Désabonnement du compte

Si un compte se retire d'une région, ses ressources apparaîtront toujours dans les résultats de recherche pendant 24 heures au maximum.

Après 24 heures, les ressources de ce compte n'apparaîtront pas dans les résultats de recherche. Pour de plus amples informations, veuillez consulter Comportements d'exclusion.

Soutenir la recherche unifiée dans AWS Management Console

AWS Management Console Il possède une barre de recherche en haut de chaque page de console. Cela fournit une expérience de recherche unifiée pour tous Services AWS. Les résultats de recherche unifiés peuvent inclure des éléments tels que :

- Service AWS et des pages de console de fonctionnalités.
- AWS pages de documentation.
- AWS articles du blog et de la base de connaissances
- Ressources dans vos comptes, si vous suivez les étapes ci-dessous.

Pour voir les ressources de votre compte dans les résultats de recherche unifiés, vous devez suivre les étapes suivantes. Vous pouvez le faire lors de la configuration initiale de Explorateur de ressources AWS. Tout se passe automatiquement si vous utilisez l'option de configuration rapide.

- Vous devez créer un index agrégateur dans un index Région AWS pour le Compte AWS.
- Vous devez créer une vue par défaut dans le Région AWS contenant l'index de l'agrégateur.
- Vous devez autoriser tous les principaux qui doivent rechercher des ressources dans la barre de recherche unifiée à utiliser cette vue par défaut.

La recherche unifiée utilise toujours la vue par défaut dans le Région AWS qui contient l'index de l'agrégateur pour effectuer toutes les recherches.

Déploiement de l'explorateur de ressources sur les comptes d'une organisation

En utilisant AWS CloudFormation StackSets, vous pouvez définir et déployer sur tous les comptes gérés dans une organisation par AWS Organizations. Lorsque vous définissez un ensemble de piles, vous spécifiez les AWS ressources que vous souhaitez créer sur votre compte cible Régions AWS et sur tous les comptes cibles que vous spécifiez. Lorsque tous les comptes font partie de la même organisation, vous pouvez tirer parti de AWS CloudFormation l'intégration avec Organizations et laisser ces services gérer la création des rôles entre comptes. Vous pouvez activer le déploiement automatique dans une organisation, qui déploie automatiquement les instances de stack sur de nouveaux comptes que vous pourriez ajouter à l'organisation cible ou à une unité organisationnelle (UO) à l'avenir. Si vous supprimez un compte de l'organisation, toutes les ressources déployées dans le cadre d'une instance de stack d'organisation sont AWS CloudFormation automatiquement supprimées. Pour plus d'informations à ce sujet StackSets, consultez la section Travailler avec AWS CloudFormation StackSets dans le guide de AWS CloudFormation l'utilisateur.

Vous pouvez l'utiliser AWS CloudFormation StackSets pour activer et configurer Explorateur de ressources AWS tous les comptes de votre organisation, en créant des index dans chaque région activée et en créant des vues là où vous en avez besoin.

> **Important**
>
> Si vous essayez de configurer un index agrégateur dans une région, vous devez vous assurer que le compte ne possède aucun index agrégateur existant dans une autre région. Après avoir rétrogradé un index agrégateur en index local, vous devez attendre 24 heures avant de pouvoir promouvoir un autre index comme nouvel index agrégateur pour le compte.

Prérequis

AWS CloudFormation StackSets Pour déployer l'Explorateur de ressources sur les comptes de votre organisation, vous, ou l'administrateur de votre organisation, devez d'abord suivre les étapes suivantes pour activer les piles avec des autorisations gérées par les services :

1. Toutes les fonctionnalités de l'organisation doivent être activées. Si seules les fonctionnalités de facturation consolidée sont activées dans l'organisation, vous ne pouvez pas créer de stack set avec des autorisations gérées par les services.

2. Activez l'accès sécurisé entre AWS CloudFormation et Organizations. Cela donne AWS CloudFormation l'autorisation de créer les rôles nécessaires dans le compte de gestion de l'organisation et les comptes membres AWS CloudFormation déploieront les index et les vues de l'explorateur de ressources.

Vous pouvez désormais créer des ensembles de piles avec des autorisations gérées par les services.

> **Important**
>
> Vous devez créer les ensembles de piles dans le compte de gestion de l'organisation. AWS CloudFormation est un service régional. Vous pouvez donc consulter et gérer les ensembles de piles que vous créez uniquement à partir de la région dans laquelle vous les avez créés à l'origine.

Création des ensembles de piles pour Resource Explorer

Pour déployer complètement l'explorateur de ressources, vous devez déployer deux ensembles de piles.

- Le premier ensemble de piles crée l'index agrégateur et la vue par défaut qui permettent aux utilisateurs de rechercher des ressources dans toutes les régions du compte.

  Déployez cet ensemble de piles uniquement dans la seule région dans laquelle vous souhaitez créer l'index agrégateur.
- Le deuxième ensemble de piles crée un index local et une vue par défaut. L'index local réplique son contenu dans l'index de l'agrégateur.

  Déployez cet ensemble de piles dans toutes les régions activées du compte, à l'exception de la région qui contient l'index agrégateur. Ne choisissez aucune région qui n'est pas activée dans les comptes sur lesquels vous déployez la pile. Si vous le faites, le déploiement échoue.

Des exemples de modèles pour chacun d'entre eux figurent dans la section suivante. Pour step-by-step obtenir des instructions sur la façon de créer un ensemble de piles à l'aide de ces modèles, voir Créer un ensemble de piles avec des autorisations gérées par des services dans le Guide de l'AWS CloudFormation utilisateur.

Une fois que vous avez déployé ces ensembles de piles dans votre organisation, chaque compte relevant du périmètre que vous avez sélectionné, organisation ou unité organisationnelle, possède un index agrégateur dans la région spécifiée et des index locaux dans toutes les autres régions.

Exemples de AWS CloudFormation modèles

L'exemple de modèle suivant crée l'index agrégateur du compte et une vue par défaut qui permet de rechercher des ressources dans toutes les régions du compte dans lequel vous déployez un index.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
    "Resources": {
        "Index": {
```

```
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

L'exemple de modèle suivant crée un index local dans chaque région activée dans tous les comptes autres que celui doté de l'index agrégateur. Il crée également une vue par défaut permettant aux utilisateurs de rechercher des ressources uniquement dans cette région. Les utilisateurs doivent effectuer une recherche à l'aide d'une vue dans la région de l'agrégateur pour rechercher des ressources dans toutes les régions.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
```

```
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
```

```
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

Désactiver l'explorateur de ressources

Lorsque vous n'avez plus besoin de rechercher des ressources dans une région spécifique Région AWS, vous pouvez les désactiver uniquement Explorateur de ressources AWS dans cette région en supprimant son index, ou vous pouvez supprimer l'explorateur de ressources dans l'ensemble Régions AWS. Lorsque vous effectuez cette opération, l'explorateur de ressources arrête de rechercher des ressources nouvelles ou mises à jour dans cette région. Si votre compte contient un index agrégateur, la réplication à partir de l'index supprimé s'arrête et les informations de l'index supprimé sont supprimées de l'index agrégateur et cessent d'apparaître dans les résultats de recherche. Jusqu'à 24 heures peuvent être nécessaires pour que toutes les ressources de l'index supprimé disparaissent des résultats de recherche dans la région contenant l'index agrégateur.

> **Note**
>
> Lorsque vous enregistrez le premier Région AWS, Resource Explorer crée un rôle lié à un service (SLR) nommé `AWSServiceRoleForResourceExplorer` dans le Compte AWS. Resource Explorer ne le supprime pas SLR automatiquement. Après avoir supprimé l'index de l'explorateur de ressources dans chaque région du compte, vous pouvez utiliser la IAM console pour le supprimer SLR si vous ne souhaitez pas utiliser l'explorateur de ressources à l'avenir. Si vous supprimez le rôle et que vous choisissez ensuite de réactiver l'Explorateur de ressources dans au moins un rôle Région AWS, Resource Explorer recrée automatiquement le rôle lié au service.

Désactiver l'explorateur de ressources en une Région AWS

Vous pouvez désactiver l'explorateur de ressources dans un en Région AWS utilisant le AWS Management Console, en utilisant les commandes dans le AWS Command Line Interface (AWS CLI), ou en utilisant API des opérations dans un AWS SDK.

Si vous désactivez l'explorateur de ressources pour un compte membre et que le membre est affiché dans une vue globale de l'organisation, il sera supprimé des résultats de recherche multi-comptes.

Si vous ne souhaitez plus prendre en charge la recherche de ressources dans un ou plusieurs des Régions AWS éléments de votre compte, effectuez les étapes de la procédure suivante.

> **Note**
>
> Si l'index que vous supprimez est l'index agrégateur du Compte AWS, vous devez attendre 24 heures avant de pouvoir promouvoir un autre index local comme index agrégateur du compte. Les utilisateurs ne peuvent pas effectuer de recherches à l'échelle du compte à l'aide de l'Explorateur de ressources tant qu'un autre index d'agrégation n'est pas configuré.

AWS Management Console

Pour supprimer l'index Resource Explorer dans un Région AWS

1. Ouvrez la page des paramètres de l'explorateur de ressources.
2. Dans la section Index, cochez les cases situées à côté Régions AWS des index que vous souhaitez supprimer, puis choisissez Supprimer.
3. Sur la page Supprimer les index, vérifiez que vous n'avez sélectionné que les index que vous souhaitez supprimer. Tapez **`delete`** dans la zone de texte Confirmer, puis choisissez Supprimer les index.

   L'explorateur de ressources affiche une bannière verte en haut de la page pour indiquer le succès, ou une bannière rouge en cas d'erreur dans une ou plusieurs des régions sélectionnées.

AWS CLI

Pour supprimer l'index Resource Explorer dans un Région AWS

Si vous ne souhaitez plus prendre en charge la recherche de ressources dans un ou plusieurs des Régions AWS éléments de votre compte, exécutez les commandes suivantes.

Exécutez la commande suivante pour chaque région contenant les index que vous souhaitez supprimer. Vous devez exécuter la commande dans la région avec l'index que vous souhaitez supprimer. L'exemple de commande suivant supprime l'index Resource Explorer dans l'ouest des États-Unis (Oregon) (`us-west-2`).

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
```

```
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

Étant donné que Resource Explorer effectue une partie du nettoyage des suppressions sous forme de tâches asynchrones en arrière-plan, la réponse peut indiquer que l'opération est le cas. `DELETING` Ce statut indique que les processus en arrière-plan ne sont pas encore terminés. Vous pouvez vérifier l'achèvement final en exécutant la commande suivante et en vérifiant si le `State` à remplacer par`DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

Désactiver l'explorateur de ressources dans tous Régions AWS

Si vous souhaitez la désactiver Explorateur de ressources AWS complètement, effectuez la procédure suivante.

> **Note**
>
> Resource Explorer crée un rôle lié à un service nommé AWSServiceRoleForResourceExplorer dans le compte lorsque vous créez un index dans le premier Région AWS pour un compte. L'explorateur de ressources ne supprime pas automatiquement ce rôle lié au service. Après avoir supprimé l'index de l'explorateur de ressources dans chaque région, vous pouvez utiliser la IAM console pour supprimer le rôle si vous êtes sûr de ne pas réutiliser l'explorateur de ressources à l'avenir. Si vous supprimez le

rôle et que vous choisissez ensuite de démarrer l'Explorateur de ressources dans au moins un rôle Région AWS, Resource Explorer recrée le rôle lié au service.

Vous pouvez désactiver l'explorateur de ressources en utilisant le AWS Management Console, en utilisant les commandes dans le AWS Command Line Interface (AWS CLI) ou en utilisant API des opérations dans un AWS SDK.

AWS Management Console

Si vous ne souhaitez plus prendre en charge la recherche de ressources Région AWS dans aucun de vos Compte AWS fichiers, effectuez les étapes de la procédure suivante.

Pour désactiver l'explorateur de ressources dans tous les cas Régions AWS

1. Ouvrez la page des paramètres de l'explorateur de ressources.
2. Dans la section Index, cochez les cases situées à côté de tous les fichiers enregistrés Régions AWS, puis choisissez Supprimer.

   > **Tip**
   >
   > Vous pouvez cocher la case dans la ligne d'en-tête du tableau à côté de Index pour cocher les cases de toutes les régions en une seule étape.

3. Sur la page Supprimer les index, vérifiez que vous souhaitez supprimer tous les index. Tapez **`delete`** dans la zone de texte Confirmer, puis choisissez Supprimer les index.

   L'explorateur de ressources affiche une bannière verte en haut de la page pour indiquer le succès, ou une bannière rouge en cas d'erreur dans une ou plusieurs des régions sélectionnées.

AWS CLI

Pour désactiver l'explorateur de ressources dans tous les cas Régions AWS

Si vous ne souhaitez plus prendre en charge la recherche de ressources Régions AWS dans aucune ressource de votre compte, exécutez la commande suivante pour trouver l'index ARN de chaque index Région AWS dans lequel vous avez précédemment activé l'Explorateur de ressources.

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd33333333"
]
```

Pour chaque réponse, exécutez la commande suivante pour supprimer l'index de l'explorateur de ressources dans cette région.

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "State": "DELETING"
}
```

Répétez la commande précédente dans chaque région supplémentaire.

Étant donné que Resource Explorer effectue une partie du nettoyage sous forme de tâches asynchrones en arrière-plan, la réponse peut indiquer que l'opération est effectuée. `DELETING` Ce statut indique que les processus en arrière-plan ne sont pas encore terminés. Vous pouvez vérifier l'achèvement final en exécutant la commande suivante et en vérifiant si le statut doit être changé`DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
```

```
}
```

Gestion des vues de l'explorateur de ressources pour fournir un accès à la recherche

Les vues sont essentielles pour rechercher vos ressources. Chaque opération Explorateur de ressources AWS de recherche doit utiliser une vue. Les vues sont la méthode que l'administrateur peut utiliser pour contrôler l'accès aux informations relatives aux ressources de votre Compte AWS.

Seuls les principaux (IAMrôles ou utilisateurs) autorisés à utiliser cette vue peuvent accéder à une vue. Pour que la recherche soit réussie avec Resource Explorer, un principal doit avoir `Allow` accès à la fois aux `resource-explorer-2:Search` opérations `resource-explorer-2:GetView` et sur la vue ARN.

Les vues contiennent des filtres intégrés que l'administrateur peut utiliser pour limiter les résultats aux seuls éléments intéressants. Par exemple, vous pouvez créer une vue qui inclut uniquement les ressources liées à un certain projet. Les utilisateurs qui n'ont pas besoin de consulter les informations relatives à d'autres projets peuvent utiliser cette vue pour voir uniquement les ressources qui les intéressent.

Une vue est une ressource régionale. La vue est créée et stockée dans une région spécifique Région AWS et renvoie dans ses résultats uniquement les informations de l'index de cette région. Pour inclure les résultats de toutes les régions dans le compte, la vue doit résider dans la région qui contient l'index agrégateur. Cette région contient une réplique des index de toutes les autres régions du compte.

Chaque point de vue comporte plusieurs éléments clés :

Autorisations de recherche

Vous pouvez utiliser des politiques AWS d'autorisation standard pour contrôler qui peut utiliser chaque vue. Cela est assuré par des politiques d'autorisation basées sur l'identité associées aux principes qui vous permettent de contrôler avec précision les personnes autorisées à consulter les informations fournies par chaque vue. Par exemple, vous pouvez autoriser l'accès à la `Production-resources` vue pour autoriser uniquement les ingénieurs qui gèrent vos services de production à effectuer des recherches. Vous pouvez ensuite accorder différentes autorisations à la `Pre-production-resources` vue afin de permettre à vos développeurs de rechercher des ressources de pré-production.

Si vous utilisez la politique AWS gérée nommée `AWSResourceExplorerReadOnlyAccess` avec vos mandants, elle leur permet d'effectuer des recherches en utilisant n'importe quel affichage du compte.

Vous pouvez également créer votre propre politique d'autorisations et accorder les autorisations suivantes uniquement pour certaines vues :

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

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 IAM via un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la section Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur.

- IAMutilisateurs :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section Création d'un rôle pour un IAM utilisateur dans le Guide de IAM l'utilisateur.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la section Ajouter des autorisations à un utilisateur (console) dans le guide de IAM l'utilisateur.

Pour plus d'informations sur les autorisations associées aux vues, consultezAutorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

Filtrer la recherche

Une vue sert de fenêtre virtuelle à travers laquelle l'utilisateur peut voir les ressources du compte. Vous pouvez créer plusieurs vues, chacune présentant une vue différente de l'image dans son ensemble. Par exemple, vous pouvez créer une vue qui permet de rechercher uniquement les ressources associées à votre environnement de pré-production, telles qu'identifiées par les balises associées à vos ressources. Vous pouvez ensuite créer une vue séparée qui permet de rechercher uniquement les ressources de votre environnement de production, en fonction des différentes valeurs des balises. Si vous configurez plusieurs vues avec des `FilterString`

valeurs différentes, il n'est pas nécessaire de saisir à nouveau ces paramètres de requête à chaque fois que vous effectuez une recherche.

Les vues peuvent également spécifier les informations facultatives sur les ressources à inclure dans les résultats. La liste de champs par défaut est toujours incluse dans les résultats. Outre la liste par défaut, vous pouvez demander que la vue inclue également les balises associées à la ressource .

Étendue de la recherche

- Étendue de la région — Lorsque vous effectuez une recherche dans un Région AWS explorateur de ressources, les résultats ne peuvent inclure que les ressources indexées dans cette région. Dans la plupart des régions, l'index est étiqueté `LOCAL` car il contient des informations sur les ressources propres à cette région uniquement. Les recherches effectuées dans ces régions ne peuvent renvoyer que ces ressources.
- Étendue du compte — Vous pouvez promouvoir un index local comme indice agrégateur du compte. Dans ce cas, toutes les autres régions dans lesquelles l'explorateur de ressources est activé répliquent leurs informations d'index dans la région avec l'index agrégateur. Si vous effectuez une recherche dans cette région, ces résultats incluent les ressources de toutes les régions du compte. Lorsque vous utilisez l'option de configuration rapide pour configurer le serveur, Resource Explorer crée automatiquement un index agrégateur dans la région que vous spécifiez. En outre, l'option de configuration rapide crée une vue par défaut dans cette région afin de faciliter la recherche de toutes les ressources du compte dans toutes les régions.

Vues par défaut

Si un utilisateur tente d'effectuer une recherche sans spécifier explicitement de vue, Resource Explorer utilise la vue par défaut définie pour cela Région AWS.

S'il n'existe pas de vue par défaut pour cette région et que l'utilisateur n'a pas indiqué de vue à utiliser, la recherche échoue et génère une exception.

Resource Explorer crée automatiquement une vue par défaut comme suit :

- Si vous activez l'Explorateur de ressources à l'aide de l'option Configuration rapide AWS Management Console et que vous choisissez l'option Configuration rapide, vous devez spécifier la région qui contient l'index agrégateur du compte. Resource Explorer crée automatiquement une vue par défaut dans la région d'index d'agrégateur spécifiée.

- Si vous enregistrez Resource Explorer à l'aide de l'option Configuration avancée AWS Management Console et que vous choisissez l'option Configuration avancée, vous pouvez éventuellement choisir de créer l'index agrégateur pour le compte dans une région spécifiée. Dans ce cas, Resource Explorer crée automatiquement une vue par défaut dans la région d'index de l'agrégateur.
- Si vous enregistrez Resource Explorer à l'aide de la console et que vous choisissez de ne pas enregistrer de région d'index agrégateur, Resource Explorer crée une vue par défaut pour l'index local dans chaque région.
- Si vous enregistrez Resource Explorer à l'aide API des opérations AWS CLI ou, Resource Explorer ne crée pas automatiquement une vue par défaut. Vous devez plutôt configurer l'affichage par défaut manuellement pour chaque région à partir de laquelle vous souhaitez que les utilisateurs effectuent des recherches.

Création de vues Resource Explorer à utiliser pour la recherche

Toutes les recherches doivent utiliser une vue. Une vue définit des filtres qui déterminent quelles ressources peuvent être renvoyées par les requêtes utilisant la vue. Les vues contrôlent également qui peut rechercher des ressources.

Une vue est stockée dans un et renvoie Région AWS les résultats de recherche uniquement à partir de l'index de cette région. Si la région contient l'index agrégateur, la vue renvoie les résultats de recherche à partir de l'index de chaque région du compte.

Les vues multicomptes vous permettent de rechercher des ressources dans les comptes de votre organisation. Tout compte dans lequel vous souhaitez effectuer une recherche nécessite des index. Seul le compte de gestion, ou un administrateur délégué de l'organisation, peut créer une vue multi-comptes.

Explorateur de ressources AWS peut créer une vue par défaut pour vous lors de la configuration initiale si vous avez choisi les options appropriées soit dans Quick Setup for Resource Explorer dans la console Systems Manager, soit dans la configuration avancée. À tout moment, vous pouvez créer des vues supplémentaires dotées de filtres différents pour différents groupes d'utilisateurs.

Vous pouvez créer une vue en utilisant AWS Management Console ou en exécutant des AWS CLI commandes ou API des opérations équivalentes dans un AWS SDK.

Autorisations minimales

Pour exécuter cette procédure, vous devez disposer des autorisations suivantes :

- Action : `resource-explorer-2:CreateView`

  Ressource : Cela peut être * pour autoriser la création d'une vue Région AWS dans n'importe quel élément du compte.

AWS Management Console

Pour créer une vue

1. Ouvrez la page Vues de la console Resource Explorer et choisissez Créer une vue.
2. Sur la page Créer une vue, dans Nom, entrez le nom de la vue.

   Le nom ne doit pas comporter plus de 64 caractères et peut inclure des lettres, des chiffres et le trait d'union (-). Le nom doit être unique au sein de son Région AWS.
3. Choisissez celui Région AWS dans lequel vous souhaitez créer la vue. Pour créer une vue qui renvoie les ressources de toutes les régions du compte, choisissez Région AWS celle qui contient l'index agrégateur.
4. (Facultatif) Pour Scope, choisissez si votre recherche renvoie des ressources multi-comptes ou renvoie uniquement des ressources provenant de votre compte. L'étendue au niveau du compte est la valeur par défaut.

   Seul le compte de gestion ou l'administrateur délégué peut voir l'option permettant de créer une vue multi-comptes.
5. Choisissez si vous souhaitez filtrer les résultats.

   - Inclure toutes les ressources

     Aucun filtre de requête n'est inclus. Toutes les ressources de l'index associé à la vue peuvent être renvoyées dans les résultats de recherche.
   - Inclure uniquement les ressources correspondant à un filtre spécifié

     Active la case à cocher Filtres de ressources dans laquelle vous pouvez choisir les noms et les opérateurs des filtres. Pour une explication de chacun des noms de filtres et opérateurs disponibles, consultezFiltres.
   - Choisissez les attributs de ressource facultatifs à inclure dans les résultats de cette vue. Cochez la case située à côté des balises pour permettre aux utilisateurs de rechercher des

ressources en fonction des noms et des valeurs de leurs clés de balise. Si vous n'incluez pas de balises dans la vue, les utilisateurs ne peuvent pas effectuer de demandes de recherche utilisant des clés et des valeurs de balise pour filtrer davantage les résultats.

- Vous pouvez éventuellement associer des balises à la vue. Développez la zone Tags et entrez jusqu'à 50 paires clé/valeur de balise. Vous pouvez utiliser des balises pour classer les ressources ou dans le cadre d'une stratégie d'autorisation de sécurité basée sur le contrôle d'accès (ABAC) basée sur les attributs. Pour de plus amples informations, veuillez consulter L'ajout d'balises aux vues.
- Choisissez Créer une vue.

La console revient à la page de recherche où vous pouvez utiliser votre nouvel affichage pour effectuer une recherche.

Étape suivante : autorisez les principaux utilisateurs de votre compte à effectuer des recherches avec votre nouvelle vue. Pour plus d'informations, consultez Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

AWS CLI

Pour créer une vue

Exécutez la commande suivante pour créer une vue dans le champ spécifié Région AWS. L'exemple suivant crée une vue qui renvoie uniquement les ressources liées au EC2 service Amazon qui sont étiquetées avec une `Stage` clé et une valeur`prod`.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
```

```
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Pour créer une vue au niveau de l'organisation

L'exemple suivant crée une vue qui renvoie des ressources provenant de l'ensemble de votre organisation. Cela doit être effectué par le compte de gestion de l'organisation ou par un compte d'administrateur délégué.

1. Exécutez la `aws organizations describe-organization` commande pour obtenir votre organisationARN.
2. Exécutez la commande suivante pour créer une vue pour l'organisation spécifiée.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Pour créer une vue au niveau de l'unité organisationnelle

L'exemple suivant crée une vue qui renvoie les ressources de tous les membres de cette unité organisationnelle. Cette vue se comporte de la même manière qu'une vue au niveau de l'organisation. Cela doit être effectué par le compte de gestion de l'organisation ou par un compte d'administrateur délégué.

1. Exécutez la `aws organizations describe-organizational-unit` commande pour obtenir votre organisationARN.
2. Exécutez la commande suivante pour créer une vue pour l'unité organisationnelle spécifiée.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Étape suivante : autorisez les principaux utilisateurs de votre compte à effectuer des recherches avec votre nouvelle vue. Pour plus d'informations, consultez Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

Autorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche

Avant que les utilisateurs puissent effectuer une recherche avec une nouvelle vue, vous devez octroyer l'accès auxExplorateur de ressources AWS vues. Pour ce faire, utilisez une politique

d'autorisation basée sur l'identité pour les principaux utilisateursAWS Identity and Access Management (IAM) qui doivent effectuer des recherches avec la vue.

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.

Vous pouvez utiliser l'une des méthodes suivantes :

- Utilisez une politiqueAWS gérée existante. L'Explorateur de ressources fournit plusieurs politiquesAWS gérées prédéfinies que vous pouvez utiliser. Pour plus de détails sur toutes les politiquesAWS gérées disponibles, consultezAWS politiques gérées pour Explorateur de ressources AWS.

  Par exemple, vous pouvez utiliser cette`AWSResourceExplorerReadOnlyAccess` politique pour accorder des autorisations de recherche à toutes les vues du compte.
- Créez votre propre politique d'autorisation et attribuez-la aux responsables. Si vous créez votre propre politique, vous pouvez restreindre l'accès à une seule vue ou à un sous-ensemble des vues disponibles en spécifiant le nom de ressource Amazon (ARN) de chaque vue dans l'`Resource`élément de la déclaration de politique. Par exemple, vous pouvez utiliser l'exemple de politique suivant pour autoriser ce principal à effectuer une recherche en utilisant uniquement cette vue.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

Utilisez la console IAM pour créer les politiques d'autorisation et les utiliser avec les principaux utilisateurs qui ont besoin de ces autorisations. Pour plus d'informations sur les stratégies d'autorisation IAM, consultez les rubriques suivantes :

- Politiques et autorisations dans IAM
- Ajout et suppression d'autorisations basées sur l'identité IAM
- Comprendre les autorisations accordées par une politique

Utiliser l'autorisation basée sur des balises pour contrôler l'accès à vos vues

Si vous choisissez de créer plusieurs vues avec des filtres qui renvoient des résultats uniquement avec certaines ressources, vous souhaiterez peut-être également restreindre l'accès à ces vues aux seules personnes qui ont besoin de consulter ces ressources. Vous pouvez fournir ce type de sécurité pour les vues de votre compte en utilisant une stratégie de contrôle d'accès basé sur les attributs (ABAC). Les attributs utilisés par ABAC sont les balises attachées à la fois aux principaux tentant d'effectuer des opérationsAWS et aux ressources auxquelles ils tentent d'accéder.

ABAC utilise des politiques d'autorisation IAM standard associées aux principes. Les politiques utilisent`Condition` des éléments contenus dans les déclarations de politique pour autoriser l'accès uniquement lorsque les balises attachées au principal demandeur et les balises attachées à la ressource affectée répondent aux exigences de la politique.

Par exemple, vous pouvez associer une étiquette`"Environment" = "Production"` à toutes lesAWS ressources qui prennent en charge l'application de production de votre entreprise. Pour vous assurer que seules les personnes autorisées à accéder à l'environnement de production peuvent accéder à ces ressources, créez une vue de l'Explorateur de ressources qui utilise cette

balise comme filtre. Ensuite, pour restreindre l'accès à la vue aux seules personnes principales appropriées, vous accordez des autorisations à l'aide d'une politique assortie d'une condition similaire aux exemples d'éléments suivants.

```
{
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

`Condition`Dans l'exemple précédent, cela indique que la demande n'est autorisée que si la`Environment` balise attachée au principal auteur de la demande correspond à la`Environment` balise attachée à la ressource spécifiée dans la demande. Si ces deux balises ne correspondent pas exactement, ou si l'une des balises est manquante, l'Explorateur de ressources refuse la demande.

> **Important**
>
> Pour utiliser ABAC avec succès afin de sécuriser l'accès à vos ressources, vous devez d'abord restreindre l'accès à la possibilité d'ajouter ou de modifier les balises associées à vos principaux et ressources. Si un utilisateur peut ajouter ou modifier les balises attachées à unAWS principal ou à une ressource, il peut affecter les autorisations contrôlées par ces balises. Dans un environnement ABAC sécurisé, seuls les administrateurs de sécurité agréés sont autorisés à ajouter ou à modifier les balises attachées aux principaux, et seuls les administrateurs de sécurité et les propriétaires de ressources peuvent ajouter ou modifier les balises associées aux ressources.

Pour plus d'informations sur la façon de mettre en œuvre avec succès une stratégie ABAC, consultez les rubriques suivantes dans le Guide de l'utilisateur IAM :

- DidididididididididididididididididididididacticielAWS
- Contrôle de l'accès auxAWS ressources à l'aide de balises

Une fois que vous avez mis en place l'infrastructure ABAC nécessaire, vous pouvez utiliser les balises pour contrôler qui peut effectuer des recherches à l'aide des vues de l'Explorateur de

ressources de votre compte. Pour des stratégies illustrant le principe, consultez les exemples de stratégies d'autorisation suivants :

- Octroi d'un accès à une vue basée sur des balises
- Autoriser l'accès à la création d'une vue basée sur des balises

Définition d'une vue par défaut dans unRégion AWS

DansExplorateur de ressources AWS, vous pouvez définir de nombreuses vues dans unRégion AWS, où chaque vue répond à différentes exigences de recherche. Nous vous recommandons de définir une vue par région comme vue par défaut pour cette région.

L'Explorateur de ressources utilise la vue par défaut chaque fois qu'un utilisateur effectue une recherche et ne spécifie pas explicitement la vue à utiliser. La barre de recherche unifiée en haut de chaqueAWS Management Console page utilise également automatiquement l'affichage par défaut de la région qui contient l'index agrégateur pour rechercher les ressources correspondant à la requête de recherche de l'utilisateur.

Vous ne pouvez sélectionner qu'une vue qui existe dans la région comme vue par défaut de cette région. Si une autre région possède une vue que vous souhaitez utiliser, vous devez d'abord créer une copie de cette vue dans la région dans laquelle vous souhaitez en faire la vue par défaut.

> **Tip**
>
> Il n'y a aucune opération de copie d'affichage. Vous devez créer une vue dans la région cible, puis copier les paramètres de la vue existante vers la nouvelle vue.

Vous pouvez spécifier une vue comme affichage par défaut pour sa région en utilisantAWS Management Console ou en exécutant desAWS CLI commandes ou leurs opérations d'API équivalentes dans unAWS SDK.

AWS Management Console

Pour définir une vue par défaut

1. Sur la page Vues de l'explorateur de ressources, cliquez sur le bouton d'option à côté de la vue que vous souhaitez définir comme valeur par défaut pour sa région.

2. Choisissez Actions, puis choisissez Définir par défaut.

AWS CLI

Pour définir une vue par défaut

Exécutez la commande suivante pour définir la vue par défaut de sa région. L'exemple suivant définit la vue spécifiée comme étant la vue par défaut pour toutes les recherches effectuées dans la région us-east-1 . Cette vue doit exister dans la région dans laquelle vous exécutez la commande.

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

L'ajout d'balises aux vues

Vous pouvez ajouter des balises à vos vues afin de les classer. Les balises sont des métadonnées fournies par le client qui prennent la forme d'une chaîne de nom de clé et d'une chaîne de valeur facultative associée. Pour des informations générales sur le balisageAWS des ressources, consultez la section MarquageAWS des ressources dans le Référence générale d'Amazon Web Services.

Ajoutez des balises à vos vues

Vous pouvez ajouter des balises à vos vues de l'Explorateur de ressources en utilisantAWS Management Console ou en exécutant desAWS CLI commandes ou leurs opérations d'API équivalentes dans unAWS SDK.

AWS Management Console

Pour ajouter des balises à une vue

1. Ouvrez la page Vues de l'Explorateur de ressources et choisissez le nom de la vue à étiqueter pour afficher sa page de détails.

2. Sous Balises, choisissez Gérer les balises.
3. Pour ajouter une balise, choisissez Ajouter la balise, puis entrez un nom de clé de balise et une valeur facultative.

   > **Note**
   >
   > Vous pouvez également supprimer un tag en cliquant sur le X à côté du tag.

   Vous pouvez attacher jusqu'à 50 balises définies par l'utilisateur à une ressource. Les balises créées et gérées automatiquement parAWS ne sont pas prises en compte dans ce quota.
4. Lorsque vous avez terminé de modifier toutes les balises, choisissez Enregistrer les modifications.

AWS CLI

Pour ajouter des balises à une vue

Exécutez la commande suivante afin d'ajouter des balises à une vue. L'exemple suivant ajoute des balises avec le nom de la clé`environment` et la valeur`production` à la vue spécifiée.

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

La commande précédente ne produit aucune sortie si elle réussit.

> **Note**
>
> Pour supprimer une étiquette existante d'une vue, utilisez la`untag-resource` commande.

Contrôle des autorisations à l'aide de balises

L'une des principales utilisations du balisage est de soutenir une stratégie de contrôle d'accès basé sur les attributs (ABAC). ABAC peut vous aider à simplifier la gestion des autorisations en vous

permettant de baliser les ressources. Ensuite, vous accordez l'autorisation aux utilisateurs d'accéder aux ressources qui sont balisées d'une certaine manière.

Par exemple, envisagez ce scénario. Pour une vue appeléeViewA, vous attachez la baliseenvironment=prod (nom de la clé = valeur). Un autreViewB pourrait être marquéeenvironment=beta. Vous balisez vos rôles et vos utilisateurs avec les mêmes balises et valeurs, en fonction de l'environnement auquel chaque rôle ou utilisateur doit pouvoir accéder.

Vous pouvez ensuite attribuer une politique d'autorisationAWS Identity and Access Management (IAM) à vos rôles, groupes et utilisateurs IAM. La politique autorise l'accès et la recherche à l'aide d'une vue uniquement si le rôle ou l'utilisateur à l'origine de la demande de recherche possède uneenvironment étiquette ayant la même valeur que laenvironment balise associée à la vue.

L'avantage de cette approche est qu'elle est dynamique et qu'elle ne vous oblige pas à tenir à jour une liste indiquant qui a accès à quelles ressources. Vous devez plutôt vous assurer que toutes les ressources (vos points de vue) et les principaux (rôles IAM et utilisateurs) sont correctement balisés. Ensuite, les autorisations sont mises à jour automatiquement sans que vous ayez à modifier les politiques.

Référencer des balises dans une politique ABAC

Une fois vos vues balisées, vous pouvez choisir d'utiliser ces balises pour contrôler l'accès dynamique à ces vues. L'exemple de politique suivant part du principe que vos principes IAM et vos vues sont balisés à l'aide de la clé de baliseenvironment et d'une valeur. Une fois que c'est fait, vous pouvez attacher l'exemple de politique suivant à vos directives. Vos rôles et utilisateurs peuvent ensuiteSearch utiliser toutes les vues balisées avec une valeur deenvironment balise qui correspond exactement à laenvironment balise associée au principal.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
```

```
                }
            }
        }
    ]
}
```

Si la balise est associée à la vue principale mais que les valeurs ne correspondent pas, ou si la`environment` balise est manquante dans l'une ou l'autre, l'`environment`Explorateur de ressources refuse la demande de recherche.

Pour plus d'informations sur l'utilisation d'ABAC pour accorder un accès sécurisé à vos ressources, voir À quoi sert ABACAWS ?

Partager les vues de l'explorateur de ressources

Les vues utilisent Explorateur de ressources AWS principalement des politiques basées sur les ressources pour accorder l'accès. À l'instar des politiques relatives aux compartiments Amazon S3, ces politiques sont associées à la vue et spécifient qui peut utiliser la vue. Cela contraste avec AWS Identity and Access Management (IAM) les politiques basées sur l'identité. Une politique IAM basée sur l'identité est attribuée à un rôle, un groupe ou un utilisateur, et elle spécifie les actions et les ressources auxquelles ce rôle, ce groupe ou cet utilisateur peut accéder. Vous pouvez utiliser l'un ou l'autre type de politique avec les vues Resource Explorer, comme suit :

- Dans le compte de gestion ou le compte d'administrateur délégué propriétaire de la ressource, utilisez l'un ou l'autre type de politique pour accorder l'accès, à condition qu'aucune autre politique ne refuse explicitement l'accès à la vue à ce principal.
- Sur tous les comptes, vous devez utiliser les deux types de politiques. La politique basée sur les ressources attachée à la vue dans le compte de partage active le partage avec un autre compte consommateur. Toutefois, cette politique n'accorde pas l'accès aux utilisateurs ou aux rôles individuels du compte consommateur. L'administrateur du compte consommateur doit également attribuer une politique basée sur l'identité aux rôles et utilisateurs souhaités dans le compte consommateur. Cette politique donne accès au nom de ressource Amazon (ARN) de la vue.

Pour partager des vues avec d'autres comptes, vous devez utiliser AWS Resource Access Manager (AWS RAM). AWS RAM gère pour vous la complexité des politiques basées sur les ressources. Avant de pouvoir partager, vous devez effectuer les tâches suivantes :

- Activez la recherche multi-comptes.

- Assurez-vous que votre politique basée sur les ressources ou la politique basée IAM sur l'identité que vous utilisez pour partager et annuler le partage des vues inclut les autorisations et. `resource-explorer-2:GetResourcePolicy` `resource-explorer-2:PutResourcePolicy` `resource-explorer-2:DeleteResourcePolicy`

Pour partager une vue, vous devez être le compte de gestion de l'organisation ou un administrateur délégué. Vous spécifiez les comptes ou les identités avec lesquels vous souhaitez partager la ressource. AWS RAM prend entièrement en charge les vues Resource Explorer. AWS RAM utilise des politiques similaires à celles décrites dans les sections suivantes, en fonction des types de principes avec lesquels vous choisissez de partager. Pour savoir comment partager des ressources, consultez la section Partage de vos AWS ressources dans le guide de AWS Resource Access Manager l'utilisateur.

Les administrateurs et les administrateurs délégués peuvent créer et partager 3 types de vues : la vue du périmètre de l'organisation, les vues du périmètre des unités organisationnelles (UO) et les vues du périmètre au niveau du compte. Ils peuvent partager avec des organisations ou des comptes. OUs Lorsque des comptes rejoignent ou quittent l'organisation, la vue partagée est AWS RAM automatiquement accordée ou révoquée.

Politique d'autorisations avec laquelle partager une vue Comptes AWS

L'exemple de politique suivant montre comment vous pouvez mettre une vue à la disposition des principaux de deux manières différentes Comptes AWS :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
```

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

L'administrateur de chacun des comptes spécifiés doit désormais spécifier quels rôles et quels utilisateurs peuvent accéder à la vue en associant des politiques d'autorisation basées sur l'identité aux rôles, aux groupes et aux utilisateurs. Les administrateurs des comptes 111122223333 ou 444455556666 peuvent créer l'exemple de politique suivant. Ils peuvent ensuite attribuer la politique aux rôles, aux groupes et aux utilisateurs de ces comptes qui doivent être autorisés à effectuer des recherches en utilisant la vue partagée depuis le compte d'origine.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

Vous pouvez utiliser ces politiques IAM basées sur l'identité dans le cadre d'une stratégie de sécurité de contrôle d'accès basé sur les attributs ()ABAC. Dans ce paradigme, vous vous assurez que toutes vos ressources et toutes vos identités sont étiquetées. Ensuite, vous spécifiez dans vos politiques quelles clés et valeurs de balise doivent correspondre entre l'identité et la ressource pour que l'accès soit autorisé. Pour plus d'informations sur le balisage des vues de votre compte, consultezL'ajout d'balises aux vues. Pour plus d'informations sur le contrôle d'accès basé sur les attributs, voir À quoi ça sert ? ABAC AWS et le contrôle de l'accès aux AWS ressources à l'aide de balises, tous deux dans le guide de IAM l'utilisateur.

Supprimer des vues dans Resource Explorer

Lorsque vous n'avez plus besoin d'uneExplorateur de ressources AWS vue, vous pouvez la supprimer. Vous pouvez supprimer des vues à l'aide de la commandeAWS Management Console ou en exécutant desAWS CLI commandes ou leurs opérations d'API équivalentes dans unAWS SDK.

> **Note**
>
> Vous ne pouvez pas supprimer une vue qui est actuellement désignée comme vue par défaut pour cette vueRégion AWS. Pour supprimer la vue, vous devez supprimer la vue par défaut. Pour ce faire, vous pouvez exécuter l'opération DisassociateDefaultViewAPI dans cette région.

Autorisations minimales

Pour exécuter cette procédure, vous devez disposer des autorisations suivantes :

- Action : `resource-explorer-2:DeleteView`

  Ressource : L'ARN de la vue à supprimer

AWS Management Console

Pour supprimer une vue

1. Sur la page Vues de la console Resource Explorer, cliquez sur le bouton d'option situé à côté de la vue que vous souhaitez supprimer.
2. Choisissez Actions, puis Delete (Supprimer).
3. Dans la boîte de dialogue de confirmation, entrez le nom de la vue, puis choisissez Delete.

AWS CLI

Pour supprimer une vue

Exécutez la commande suivante pour supprimer la vue avec l'ARN (Amazon Resource Name) spécifié.

```
$ aws resource-explorer-2 delete-view \
```

```
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

En utilisantExplorateur de ressources AWSpour rechercher des ressources

L'objectif principal de permettreExplorateur de ressources AWSdans votreCompte AWSpermet à vos utilisateurs de rechercher des ressources dans le compte. Utilisez leAWS Management Consoleou leAWS Command Line Interface(AWS CLI) pour rechercher des ressources à l'aide de l'Explorateur de ressources.

Voici quelques-unes des principales caractéristiques de la recherche dans l'Explorateur de ressources.

- Chaque recherche doit utiliser une vue.

  La vue est utilisée par l'Explorateur de ressources pour déterminer qui est autorisé à voir quelles ressources. Pour utiliser une vue dans une opération de recherche dans l'Explorateur de ressources, l'utilisateur doit disposer d'un`Allow`sur le`resource-explorer-2:Search`opération pour la vue spécifiée. Cette autorisation provient d'unpolitique d'autorisation basée sur l'identitéattaché au principal auteur de la demande.

  La vue peut inclure un filtre qui limite les ressources pouvant être incluses dans les résultats. En créant différentes vues qui utilisent des filtres et en accordant à différents principaux utilisateurs l'accès à différentes vues, vous pouvez configurer un environnement dans lequel chaque groupe d'utilisateurs ne peut voir que les ressources qui le concernent.

  Pour plus d'informations sur les vues, voirGestion des vues de l'explorateur de ressources pour fournir un accès à la recherche.
- Resource Explorer utilise des processus d'arrière-plan asynchrones pour gérer ses index.

  Les processus d'indexation de Resource Explorer peuvent mettre un certain temps à découvrir les ressources récemment créées ou modifiées et à les ajouter à l'index local. Resource Explorer peut mettre plus de temps à répliquer les modifications des index locaux vers l'index agrégateur.

  Il en va de même pour les ressources que vous supprimez. Il peut s'écouler un certain temps après la suppression d'une ressource avant que cette suppression soit découverte par le processus d'indexation et que les informations relatives à cette ressource soient supprimées de l'index local. Resource Explorer a besoin de plus de temps pour répliquer cette suppression de l'index local vers l'index agrégateur du compte.

Les ajouts, modifications et suppressions apportés à vos ressources peuvent prendre jusqu'à 36 heures pour que Resource Explorer affiche ces modifications dans les résultats de recherche dans toutes les régions où vous avez activé Resource Explorer.

- Une recherche dans l'Explorateur de ressources s'effectue dans unRégion AWS.

  Chaque région dans laquelle vous activez l'Explorateur de ressources contient un index contenant uniquement les ressources stockées dans cette région. Les vues sont également associées à des régions et ne peuvent renvoyer que les ressources trouvées dans l'index de cette région. La seule exception à cette règle est l'index agrégateur, qui reçoit une copie répliquée de tous les index locaux afin de permettre la recherche dans toutes les régions du compte.

- La recherche interrégionale nécessite un index agrégateur pour le compte.

  Pour permettre aux utilisateurs de rechercher des ressources dans tousRégions AWS, l'administrateur doit désigner une région pour contenir l'index agrégateur du compte. Une copie de chaque index local est automatiquement répliquée vers l'index agrégateur.

  De ce fait, seules les vues de l'index d'agrégateur Region peuvent renvoyer des résultats qui incluent des ressources provenant de tousRégions AWSdans le compte.

- Une requête se compose d'un certain nombre de mots-clés et de filtres de type texte libre.

  Les mots-clés de forme libre sont combinés dans la requête à l'aide de la logique**OR**opérateurs. Filtres utilisant des noms de filtres définis par Resource Explorersont combinés dans la requête à l'aide de la logique**AND**opérateurs. Examinez l'exemple de requête suivant.

  ```
  test instance service:EC2 region:us-west-2
  ```

  Ceci est évalué par Resource Explorer comme suit.

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  Cette requête nécessite que les ressources correspondantes soient des ressources Amazon EC2 de la région USA Ouest (Oregon) et qu'elles comportent au moins l'un des mots clés (test,exemple) attachés d'une manière ou d'une autre, par exemple dans le nom, la description ou les balises.

> **Note**
>
> À cause de l'impliciteAND, vous ne pouvez utiliser avec succès qu'un seul filtre pour un attribut auquel une seule valeur peut être associée à la ressource. Par exemple, une ressource ne peut faire partie que d'uneRégion AWS. Par conséquent, la requête suivante ne renvoie aucun résultat.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Cette limitation faitpass'appliquent aux filtres pour les attributs qui peuvent avoir plusieurs valeurs en même temps, tels que`tag:`,`tag.key:`, et`tag.value:`.

- Une recherche ne peut renvoyer que les 1 000 premiers résultats.

  Cette exigence inclut une recherche avec une chaîne de requête vide correspondant à toutes les ressources. Pour voir les ressources au-delà des 1 000 renvoyées par une chaîne de requête vide, vous devez utiliser des requêtes pour restreindre les résultats correspondants à ceux que vous souhaitez voir et limiter le nombre de correspondances à moins de 1 000.
- Le nombre d'opérations de recherche que vous pouvez effectuer est limité par compte.

  Les quotas limitent le nombre de requêtes que vous pouvez effectuer par seconde et le nombre de requêtes que vous pouvez effectuer chaque mois. Pour des numéros de quotas spécifiques, voirQuotas pour Resource Explorer.

AWS Management Console

Pour rechercher des ressources à l'aide de l'Explorateur de ressources

1. Sur leRecherche de ressourcespage, commencez par choisir la vue que vous souhaitez utiliser. Vous pouvez choisir uniquement les vues auxquelles vous êtes autorisé à accéder.
2. PourRequête, entrez les termes de recherche etfiltresqui identifient les ressources que vous souhaitez consulter. Pour plus d'informations sur toutes les options de syntaxe disponibles, voirRéférence syntaxique des requêtes de recherche pour Resource Explorer.
3. PresseEntrezpour soumettre votre requête.

   L'Explorateur de ressources affiche tous les résultats qui correspondent à la fois au`Filter`défini dans la vue et dansRequêteque vous fournissez. Les résultats sont triés

par pertinence. Les ressources qui correspondent à un plus grand nombre de termes de votre requête apparaissent en haut de la liste et les ressources qui correspondent à moins de termes apparaissent plus bas dans la liste.

4. Choisissez l'identifiant d'une ressource pour accéder à la console native de ce type de ressource, où vous pouvez interagir avec la ressource de toutes les manières prises en charge par ce service.

AWS CLI

Pour rechercher des ressources à l'aide de l'Explorateur de ressources

Exécutez la commande suivante pour rechercher des ressources à l'aide de la vue spécifiée. Cette vue doit exister dans la région dans laquelle vous exécutez l'opération. L'exemple suivant recherche les instances Amazon EC2 qui sont balisées.`env=production`dans l'est des États-Unis (Ohio) (us-east-2). Pour plus d'informations sur toutes les options de syntaxe disponibles pour`query-string`paramètre, voirRéférence syntaxique des requêtes de recherche pour Resource Explorer.

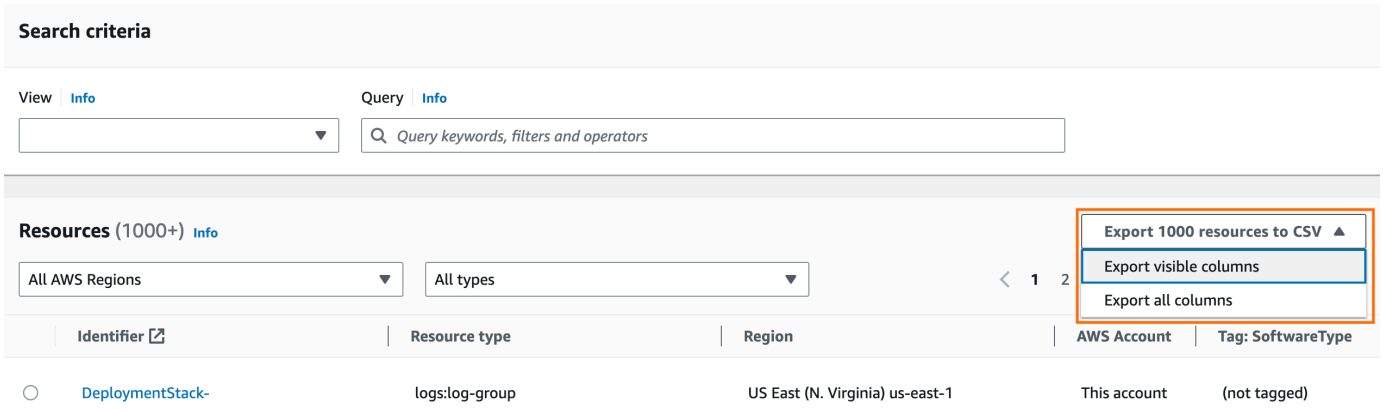
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Exporter les résultats de recherche vers un fichier .csv

Vous pouvez exporter les résultats d'unRecherche de ressourcesrequête vers un fichier de valeurs séparées par des virgules (.csv). Le fichier .csv inclut l'identifiant, le type de ressource, la région,Compte AWS, le nombre total de balises et une colonne pour chaque clé de balise unique de la collection. Le fichier .csv peut vous aider à configurer votreAWSles ressources de votre organisation, ou déterminez les chevauchements ou les incohérences dans le balisage des ressources.

1. Dans les résultats de votreRecherche de ressourcesrequête, choisissezExporter les ressources au format CSV.

   Vous pouvez choisir d'exporter vos résultats uniquement avec les colonnes que vous pouvez voir actuellement ou de les exporter avec toutes les colonnes disponibles.



2. Lorsque votre navigateur vous y invite, choisissez d'ouvrir le fichier .csv ou enregistrez-le à un emplacement approprié.

Types de ressources que vous pouvez rechercher avec Resource Explorer

Resource Explorer prend en charge les types de ressources dans de nombreux AWS services.

Rubriques

Certains types de ressources sont identifiés par des chaînes de nom de ressource Amazon (ARN) qui partagent un format commun avec un autre type de ressource. Dans ce cas, Resource Explorer peut signaler ces ressources comme cet autre type de ressource. Pour obtenir la liste des types de ressources concernés par ce problème, consultezTypes de ressources qui apparaissent sous la forme d'autres types.

Pour le moment, les balises associées aux ressources AWS Identity and Access Management (IAM), telles que les rôles ou les utilisateurs, ne peuvent pas être utilisées pour la recherche.

Si vous avez un accès chiffré à certaines de vos ressources, Resource Explorer ne peut pas les découvrir. Vous ne verrez pas ces ressources dans les résultats de recherche.

Les tableaux suivants répertorient les types de ressources pris en charge pour la recherche Explorateur de ressources AWS.

> **Note**
>
> Depuis le 9 juillet 2024, Resource Explorer ne prend plus en charge les types de ressources suivants :
>
> - Amazon Elastic Container Service — `ecs:task`
> - AWS Systems Manager — `ssm:automation-execution`
> - AWS Systems Manager — `ssm:patchbaseline`

Vous pouvez toujours utiliser ces types de ressources dans leurs propres services, mais ils ne sont plus indexés ni consultables dans Resource Explorer.

Services et types de ressources pris en charge

Soutenu Services AWS

- APIPasserelle Amazon
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Backup
- AWS Batch
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon, CloudWatch évidemment
- Amazon CloudWatch Logs
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom
- Amazon Detective

- Amazon DynamoDB
- EC2Image Builder
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (AmazonEC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR sans serveur
- Amazon EventBridge
- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise

- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- Amazon Service géré pour Apache Flink
- Amazon Managed Service for Prometheus
- Amazon Managed Service for Prometheus
- Amazon Managed Streaming for Apache Kafka
- AWS Migration Hub Refactor Spaces
- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch Service
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (AmazonRDS)
- AWS Resilience Hub
- AWS Resource Groups
- Explorateur de ressources AWS
- Amazon Route 53

- Amazon Route 53 Recovery Readiness
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- Accès vérifié par AWS
- AWS Wavelength

APIPasserelle Amazon

- `apigateway:restapis`

AWS App Runner

- `apprunner:vpcconnector`

Amazon AppStream 2.0

- `appstream:appblock`
- `appstream:application`
- `appstream:fleet`
- `appstream:stack`

AWS AppSync

- `appsync:apis`

Amazon Athena

- athena:datacatalog
- athena:workgroup

AWS Backup

- backup:backupplan

AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

AWS CloudFormation

- cloudformation:stack
- cloudformation:stackset

Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

AWS CloudTrail

- cloudtrail:trail

Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

Amazon, CloudWatch évidemment

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

Amazon CloudWatch Logs

- logs:destination
- logs:log-group

AWS CodeArtifact

- codeartifact:domain
- codeartifact:repository

AWS CodeBuild

- codebuild:project

AWS CodeCommit

- codecommit:repository

Amazon CodeGuru Profiler

- codeguru-profiler:profilingGroup

AWS CodePipeline

- codepipeline:pipeline

AWS CodeConnections

- codestarconnections:connect

Amazon Cognito

- cognito:identitypool
- cognito:userpool

Amazon Connect

- appintegrations:eventintegration

Amazon Connect Wisdom

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

Amazon Detective

- detective:graph

Amazon DynamoDB

- dynamodb:table

EC2Image Builder

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image
- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

Amazon ECR Public

- ecrpublic:repository

AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup

- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

Amazon Elastic Compute Cloud (AmazonEC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip
- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2

- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request
- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table

- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

Amazon Elastic Container Registry

- ecr:repository

Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service
- ecs:task-definition
- ecs:task-set

Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

Elastic Load Balancing

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app

- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

Amazon EMR sans serveur

- emr-serverless:applications

Amazon EventBridge

- events:event-bus
- events:rule

AWS Fault Injection Service

- fis:experimenttemplate

Amazon Forecast

- forcast:dataset

- forcast:dataset-group

Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

Amazon GameLift

- gamelift:alias

AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

AWS Glue DataBrew

- databrew:dataset
- databrew:recipe

- databrew:ruleset

AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

AWS Key Management Service

- kms:key

Amazon Kinesis

- kinesis:stream

Amazon Data Firehose

- kinesisfirehose:deliverystream

Amazon Kinesis Video Streams

- kinesisvideo:stream

AWS Lambda

- lambda:code-signing-config
- lambda:event-source-mapping
- lambda:function

Amazon Lex

- lex:bot

Amazon Location Service

- geo:place-index
- geo:tracker

Amazon Lookout for Metrics

- lookoutmetrics:Alert

Amazon Lookout for Vision

- lookoutvision:project

Amazon Service géré pour Apache Flink

- kinesisanalytics:application

Amazon Managed Service for Prometheus

- aps:rulegroupsnamespace
- aps:workspace

Amazon Managed Service for Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

Amazon Managed Streaming for Apache Kafka

- kafka:cluster
- kafka:configuration

AWS Migration Hub Refactor Spaces

- refactor-spaces:environment
- refactor-spaces:environment/application
- refactor-spaces:environment/application/route
- refactor-spaces:environment/application/service

AWS Network Firewall

- network-firewall:firewall-policy

AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

Amazon OpenSearch Service

- es:domain

AWS Panorama

- panorama:package

Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

AWS Private Certificate Authority

- acmpca:certificateauthority

Amazon QLDB

- qldb:ledger
- qldb:stream

Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

Amazon Rekognition

- rekognition:project

Amazon Relational Database Service (AmazonRDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg

- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

AWS Resilience Hub

- resiliencehub:resiliencypolicy

AWS Resource Groups

- resourcegroups:group

Explorateur de ressources AWS

- resource-explorer-2:index
- resource-explorer-2:view

Amazon Route 53

- route53:healthcheck
- route53:hostedzone

Amazon Route 53 Recovery Readiness

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint

- route53resolver:resolverrule

Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

AWS Secrets Manager

- secretsmanager:secret

AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

Amazon Simple Notification Service

- sns:topic

Amazon Simple Queue Service

- sqs:queue

Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

AWS Step Functions

- states:statemachine

- `stepfunctions:activity`

AWS Systems Manager

- `ssm:association`
- `ssm:document`
- `ssm:maintenancewindow`
- `ssm:managed-instance`
- `ssm:parameter`
- `ssm:resourcedatasync`
- `ssm:windowtarget`
- `ssm:windowtask`

Accès vérifié par AWS

- `ec2:verifiedaccessendpoint`
- `ec2:verifiedaccessgroup`
- `ec2:verifiedaccessinstance`
- `ec2:verifiedaccesstrustprovider`

AWS Wavelength

- `ec2:carriergateway`

Accès par programmation à la liste des types de ressources pris en charge

Pour accéder à la liste des types de ressources pris en charge à partir du code, vous pouvez appeler l'ListSupportedResourceTypesopération depuis n'importe quel code AWS SDK.

Par exemple, vous pouvez exécuter la commande list-supported-resource-types AWS Command Line Interface (AWS CLI), comme indiqué dans l'exemple suivant.

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

Types de ressources qui apparaissent sous la forme d'autres types

Certains types de ressources sont identifiés par des chaînes de nom de ressource Amazon (ARN) qui partagent un format commun avec un autre type de ressource. Dans ce cas, Resource Explorer peut signaler ces ressources comme cet autre type de ressource. Cela affecte les types de ressources présentés dans le tableau suivant.

Type de ressource réel	Signalé en tant que type de ressource

`ec2:securitygroupegress`
 	
`ec2:securitygroupingress`
	`ec2:security-group-rule`

`elasticloadbalancingv2:loadbalancer`	`elasticloadbalancing:loadbalancer`

`docdb:dbcluster`
 	
`neptune:dbcluster`
 	
`rds:dbcluster`
	`rds:cluster`

`docdb:dbclusterparametergroup`	`rds:cluster-pg`

Type de ressource réel	Signalé en tant que type de ressource
neptune:dbclusterparametergroup rds:dbclusterparametergroup	
docdb:clustersnapshot neptune:dbclustersnapshot rds:clustersnapshot	rds:cluster-snapshot
docdb:dbinstance neptune:dbinstance rds:dbinstance	rds:db
docdb:eventsubscription neptune:eventsubscription rds:eventsubscription	rds:es
docdb:globalcluster rds:globalcluster	rds:global-cluster
neptune:dbparametergroup rds:dbparametergroup	rds:pg
docdb:dbsubnetgroup neptune:dbsubnetgroup rds:dbsubnetgroup	rds:subgrp

Référence syntaxique des requêtes de recherche pour Resource Explorer

Explorateur de ressources AWS vous aide à trouver des AWS ressources individuelles dans votre Comptes AWS. Pour vous aider à trouver les ressources exactes que vous recherchez, Resource Explorer accepte les chaînes de requête de recherche qui prennent en charge la syntaxe décrite dans cette rubrique. Par exemple, des requêtes qui montrent comment utiliser les fonctionnalités décrites ici, voirExemples de requêtes de recherche dans Resource Explorer.

> **Note**
>
> Pour le moment, les balises associées aux ressources AWS Identity and Access Management (IAM), telles que les rôles ou les utilisateurs, ne sont pas indexées.

Fonctionnement des requêtes dans Resource Explorer

Les requêtes de recherche utilisent toujours une vue. Si vous n'en spécifiez pas explicitement une, Resource Explorer utilise la vue désignée par défaut pour la vue dans Région AWS laquelle vous travaillez.

Les vues déterminent les ressources que vous pouvez consulter. Vous pouvez créer différentes vues qui renvoient chacune un ensemble de ressources différent.

Par exemple, vous pouvez créer une vue qui inclut uniquement les ressources étiquetées avec la clé `Environment` et la valeur`Production`. Vous pouvez ensuite choisir d'accorder l'accès à cette vue uniquement aux utilisateurs qui ont des raisons professionnelles de consulter ces ressources. Les `Alpha` différents utilisateurs qui ont besoin de consulter ces ressources peuvent accéder à une vue distincte qui inclut les ressources de l'`Beta`environnement. Pour plus d'informations sur le contrôle des utilisateurs ayant accès à quelles vues, consultezAutorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche.

Syntaxe des chaînes de requête

Cette section fournit des informations sur les aspects de base de la syntaxe des requêtes, des filtres et des opérateurs de filtre.

Principes de base

Dans sa forme la plus élémentaire, a `QueryString` est un ensemble de mots clés de texte de forme libre qui sont implicitement joints par un opérateur logique**OR**. Séparez chaque mot clé des autres en utilisant un espace, comme illustré dans l'exemple suivant :

```
ec2 billing test gamma
```

Resource Explorer estime que cette liste de mots clés signifie :

```
ec2 OR billing OR test OR gamma
```

L'explorateur de ressources trie les résultats par pertinence, en privilégiant les ressources qui correspondent à un plus grand nombre de termes de recherche. Les ressources qui ne correspondent pas à un ou plusieurs termes ne sont pas exclues des résultats. Cependant, Resource Explorer les considère comme moins pertinentes et les place plus bas dans les résultats de recherche.

Si vous spécifiez une chaîne vide pour le `QueryString` paramètre, votre requête renvoie les 1 000 premières ressources disponibles via la vue utilisée pour l'opération. Le nombre maximum de ressources pouvant être renvoyées par une requête est de 1 000.

> **Note**
>
> AWS se réserve le droit de mettre à jour la logique de correspondance et les algorithmes de pertinence pour évaluer les mots clés en texte libre afin de fournir aux clients les résultats les plus pertinents. Par conséquent, les résultats renvoyés pour les mêmes requêtes utilisant des mots clés en texte libre peuvent changer au fil du temps. Lorsque vous avez besoin de résultats plus déterministes, nous vous recommandons d'utiliser des filtres. La logique de correspondance des filtres ne change pas au fil du temps.

Filtres

Vous pouvez limiter les résultats de votre requête de manière plus stricte en incluant des filtres. Contrairement aux mots clés textuels, les filtres sont évalués dans la requête à l'aide de l'ANDopérateur. Par exemple, considérez la requête suivante composée de deux mots clés libres et de deux filtres :

```
test instance service:EC2 region:us-west-2
```

Cette requête est évaluée comme suit :

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

Les filtres sont toujours évalués à l'aide d'opérateurs ANDlogiques. Si une ressource ne correspond pas au filtre, elle n'est pas incluse dans les résultats. Les résultats de l'exemple de requête incluent toutes les ressources associées à AmazonEC2, situées dans l'ouest des États-Unis (Oregon) Région AWS et auxquelles au moins un des mots clés est attaché d'une manière ou d'une autre.

> **Note**
>
> En raison de l'impliciteAND, vous ne pouvez utiliser qu'un seul filtre pour un attribut qui ne peut avoir qu'une seule valeur associée à la ressource. Par exemple, une ressource ne peut faire partie que d'une seule ressource Région AWS. Par conséquent, la requête suivante ne renvoie aucun résultat.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Cette limitation ne s'applique pas aux filtres pour les attributs qui peuvent avoir plusieurs valeurs en même temps, tels que `tag:tag.key:`, et`tag.value:`.

Le tableau suivant répertorie les noms de filtres disponibles que vous pouvez utiliser dans une requête de recherche de l'explorateur de ressources.

Nom du filtre	Description et exemple
`accountid:`	Celui Compte AWS qui possède la ressource. L'explorateur de ressources inclut dans les résultats uniquement les ressources détenues par le compte spécifié. `accountid:123456789012`
`applicati on:`	Ce filtre vous permet de rechercher des ressources avec une clé de `awsApplication` balise et une valeur de groupe de ressources. Vous

Nom du filtre	Description et exemple

	pouvez effectuer une recherche par nom d'application ou par groupe de ressources d'applicationsARN.
	
	`application:MyApplicationName`
	
	`application:arn:aws:resource-groups:  us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	`arn:aws:resource-groups:  us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	Note
	Pour utiliser ce filtre, votre vue doit avoir accès aux données de balisage.

`id:`	L'identifiant d'une ressource individuelle, exprimé sous la forme d'un nom de ressource Amazon (ARN). `id:arn:aws:license-manager:  us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE`

Nom du filtre	Description et exemple
`region:`	L' Région AWS endroit où se trouve la ressource. L'explorateur de ressources inclut dans les résultats uniquement les ressources qui résident dans le fichier spécifié Région AWS. `region:us-east-1` **Note** La saisie uniquement du code de région (sans filtre, par exemple`us-east-1`) ne renvoie pas les mêmes résultats que`region:us-east-1` . Ce résultat est dû au fait que, en tant que mot clé de texte libre qui n'est pas un filtre, le code de région est décomposé en plusieurs parties. Par exemple, `us-east-1` est recherché sous la forme `useast`, et`1`. Cette décomposition en composants ne se produit pas lorsque vous utilisez le `region:` préfixe.
`region:global`	Cas particulier pour le `region:` filtre que vous pouvez utiliser pour rechercher des ressources qui ne sont pas associées à un individu Région AWS mais dont la portée est considérée comme globale. `region:global` **Note** Le fait de taper uniquement le mot clé `global` ne renvoie pas les mêmes résultats `region:global` car le mot littéral « global » n'est pas associé aux ressources globales. La saisie `global` en tant que mot-clé renvoie uniquement les ressources auxquelles cette chaîne littérale est associée.
`resourcetype:`	Type de ressource en *`service`*`:`*`type`* notation. L'explorateur de ressources inclut dans les résultats uniquement les ressources du type spécifié. `resourcetype:ec2:instance`

Nom du filtre	Description et exemple
`resourcetype.supports:`	Ce filtre vous permet de rechercher des ressources compatibles avec les balises. `tags`est la seule valeur prise en charge. L'explorateur de ressources inclut dans les résultats uniquement les ressources pouvant être balisées. `resourcetype.supports:tags`
`service:`	Le Service AWS qui est associé au type de ressource. L'explorateur de ressources inclut dans les résultats uniquement les ressources créées et gérées par le service spécifié. `service:ec2`
`tag:`	Une paire clé/valeur de balise exprimée sous la forme. `<key>=<value>` L'explorateur de ressources inclut dans les résultats uniquement les ressources dotées d'une balise comportant à la fois une clé correspondante et la valeur spécifiée. `tag:environment=production`
`tag:all`	Cas particulier du `tag:` filtre qui vous permet de rechercher des ressources associées à une ou plusieurs balises créées par l'utilisateur, même si le type de ressource n'est pas pris en charge dans Resource Explorer. **Note** Les ressources dotées de balises AWS créées par un service apparaissent toujours dans les résultats de ce filtre.
`tag:none`	Cas particulier du `tag:` filtre qui vous permet de rechercher toutes les ressources auxquelles aucune balise créée par l'utilisateur n'est attachée. **Note** Les ressources dotées de balises AWS créées par un service apparaissent toujours dans les résultats de ce filtre.

Nom du filtre	Description et exemple
`tag.key:`	Une clé de tag. L'explorateur de ressources inclut dans les résultats uniquement les ressources dotées d'une balise avec une clé correspondante, quelle que soit leur valeur. `tag.key:environment`
`tag.value:`	Une valeur de balise. L'explorateur de ressources inclut dans les résultats uniquement les ressources dotées d'une balise avec une valeur correspon dante, quel que soit le nom de la clé. `tag.value:production`

Opérateurs de filtrage

Vous pouvez modifier vos mots clés et vos filtres en incluant l'un des opérateurs présentés dans le tableau suivant dans la chaîne.

Opérateur	Description et exemple

`"multiple word phrase"`
 	
or
 	
`"hyphenate d-phrase "`
	Entourez une phrase comportant plusieurs mots qui doit être traitée comme un seul mot clé par des guillemets doubles (`"  "`). L'explorateur de ressources inclut uniquement les ressources qui correspondent à la phrase complète, avec tous les mots ensemble et dans l'ordre spécifié.
	
	Si vous n'utilisez pas de guillemets doubles, Resource Explorer divise la phrase en ses composants par des espaces ou des tirets, et inclut les ressources correspondant aux composants individuels, même s'ils ne sont pas ensemble ou dans un ordre différent. Les devis doivent porter sur tout ce qui concerne l'opérateur.
	
	`"This matches only resources with the whole sentence."`
	
	`This matches resources with any of the words.`
	
	`"us-east-1"` — ne correspond qu'aux ressources associées à cette région précise.

Opérateur	Description et exemple
	`us-east-1` — correspond à toute ressource contenant « nous », « est » ou « 1 ». `-tag:"environment=production"`
keyword`*`	Correspondance des préfixes avec caractères génériques. Vous pouvez placer un caractère générique (un astérisque*) uniquement à la fin de la chaîne. L'explorateur de ressources inclut dans les résultats uniquement les ressources dont les valeurs commencent par le texte du préfixe situé avant le*. L'exemple suivant correspond à tout Régions AWS ce qui commence par`us-east`. `region:us-east*` **Important** La recherche unifiée insère automatiquement un opérateur de caractère générique (*) à la fin du premier mot clé de la chaîne. Cela signifie que les résultats de recherche unifiés incluent des ressource s correspondant à n'importe quelle chaîne commençant par le mot clé spécifié. La recherche effectuée par la zone de texte Requête sur la page de recherche de ressources de la console Resource Explorer n'ajoute pas automatiquement de caractère générique. Vous pouvez insérer un * manuellement après n'importe quel terme dans la chaîne de recherche.

Opérateur	Description et exemple

-keyword	Notopérateur. Vous pouvez placer un tiret (-) au début de son mot clé ou filtrer pour inverser les résultats de recherche. L'explorateur de ressources exclut des résultats toutes les ressources correspondant au mot-clé ou au filtre qui suit cet opérateur. Dans l'exemple suivant, toutes les ressources associées au EC2 service Amazon sont exclues des résultats.
	
	`-service:ec2`
	
	Important
	
	Si vous utilisez la AWS CLI `search` commande et que la valeur de votre `--query-string` paramètre comporte l'-opérateur comme premier caractère, vous devez séparer le nom du paramètre de sa valeur par un caractère de signe égal (=) au lieu du caractère espace habituel. Si vous utilisez le caractère espace, la chaîne est CLI mal interprétée. Par exemple, la requête suivante échoue.
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	La chaîne de requête corrigée suivante, avec un espace de = remplacement, fonctionne comme prévu.
	
	`aws resource-explorer-2 search --query-string ="-tag:none region:us-east-1"`
	
	Si vous modifiez l'ordre des filtres dans la chaîne de requête afin qu'il ne s'-agisse pas du premier caractère de la valeur du paramètre, vous pouvez utiliser le caractère d'espace standard. La chaîne de requête suivante fonctionne.
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

Opérateur	Description et exemple

`\<special character>`	Vous pouvez éviter les caractères spéciaux qui doivent être inclus exactement comme indiqué plutôt que interprétés. Si votre texte contient l'un des caractère s spéciaux (`* " - : = \`), vous devez le faire précéder d'une barre oblique inverse (\) pour vous assurer qu'il est pris au pied de la lettre. L'exemple suivant montre comment utiliser un mot-clé de texte libre qui inclut le caractère tiret (-) (). `"my-key-word"`
	
	En outre, pour empêcher Resource Explorer de diviser l'expression au niveau des traits d'union en trois mots clés distincts, vous pouvez placer la phrase entière entre guillemets doubles.
	
	`"my\-key\-word"`
	
	Pour insérer une barre oblique inverse littérale, insérez deux barres obliques inversées d'affilée. La première barre oblique inverse est interprétée comme un échappement et la seconde est le caractère littéral à insérer.
	
	`"some_text\\some_more_text"`

> **Note**
>
> Si la vue inclut les balises associées aux ressources, l'`Search`opération ne génère pas d'erreurs de validation pour les chaînes de recherche, car un filtre non valide peut également être interprété comme une recherche de texte libre. Par exemple, même s'il `cat:blue` ressemble à un filtre, Resource Explorer ne peut pas l'analyser comme tel car il `cat:` ne fait pas partie des filtres définis et valides. Resource Explorer interprète plutôt la chaîne entière comme une chaîne de recherche de forme libre pour lui permettre de correspondre à des éléments tels que le nom d'une clé de balise ou une partie d'un. ARN
> L'opération génère une erreur de validation si l'une des conditions suivantes est vraie :
>
> - La vue n'inclut pas d'informations sur les balises
> - La requête de recherche utilise explicitement un filtre de balises (`tag.key:`, `tag.value:`, `outag:`)

Exemples de requêtes de recherche dans Resource Explorer

Les exemples suivants montrent la syntaxe des types courants de requêtes que vous pouvez utiliser dansExplorateur de ressources AWS.

Important

Si vous utilisez laAWS CLI`search` commande et que la valeur de votre`--query-string` paramètre contient l'`-`opérateur comme premier caractère, vous devez séparer le nom du paramètre de sa valeur par un signe égal (=) au lieu de l'espace habituel. Si vous utilisez le caractère d'espace, la CLI interprète mal la chaîne. Par exemple, la requête suivante échoue.

```
aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
```

La requête corrigée suivante, en= remplaçant l'espace, fonctionne comme prévu.

```
aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
```

Si vous modifiez l'ordre des filtres dans la chaîne de requête afin que ce ne`-` soit pas le premier caractère de la valeur du paramètre, vous pouvez utiliser le caractère d'espace standard. La requête suivante fonctionne.

```
aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
```

Rechercher des ressources non balisées

Si vous souhaitez utiliser le contrôle d'accès basé sur les attributs (ABAC) sur votre compte, utiliser une allocation basée sur les coûts ou effectuer une automatisation basée sur des balises pour vos ressources, vous devez savoir quelles ressources de votre compte peuvent ne pas comporter de balises. L'exemple de requête suivant utilise la balise de filtre case spéciale : none pour renvoyer toutes les ressources pour lesquelles il manque des balises générées par l'utilisateur.

L`etag:none` filtre s'applique uniquement aux balises créées par l'utilisateur. Les balises générées et gérées parAWS sont exemptées de ce filtre et apparaissent toujours dans les résultats.

```
tag:none
```

Pour exclure également toutes les balises systèmeAWS créées, ajoutez un deuxième filtre, comme indiqué dans l'exemple suivant. Le premier élément de la chaîne de requête reproduit l'exemple précédent en filtrant toutes les balises créées par l'utilisateur. AWSles balises système créées commencent toujours par les lettres`aws`. Par conséquent, vous pouvez utiliser l'opérateur logique NOT (-) avec le filtre tag.key pour exclure également toutes les ressources dont la balise porte un nom de clé commençant par`aws`.

```
tag:none -tag.key:aws*
```

Rechercher des ressources étiquetées

Pour trouver toutes les ressources dotées d'une balise de n'importe quel type, vous pouvez utiliser l'opérateur logique NOT (-) avec le filtre case spécial : none comme suit.

```
-tag:none
```

Rechercher des ressources pour lesquelles il manque un tag spécifique

Également lié à ABAC, vous souhaiterez peut-être rechercher toutes les ressources qui n'ont pas de balise avec une clé spécifiée. L'exemple suivant utilise l'opérateur logique NOT`-` pour renvoyer toutes les ressources pour lesquelles il manque une balise avec le nom de clé`Department`.

```
-tag.key:Department
```

Rechercher des ressources dont les valeurs de balise ne sont pas valides

Pour des raisons de conformité, vous souhaiterez peut-être rechercher toutes les ressources dont les balises importantes sont manquantes ou mal orthographiées. L'exemple suivant renvoie toutes les ressources dont la balise porte le nom de clé`environment`. Toutefois, la requête filtre

toute ressource possédant l'une des valeurs validesprodinteg, oudev. Tous les résultats qui apparaissent à partir de cette requête ont une autre valeur que vous devez étudier et corriger.

> **Important**
>
> Les recherches dans l'Explorateur de ressources ne distinguent pas les majuscules des majuscules et ne permettent pas de faire la distinction entre les noms de clés et les valeurs qui ne diffèrent que par la façon dont ils sont mis en majuscules. Par exemple, les valeurs de l'exemple suivant correspondent àPR0D,prodPr0d, ou à une variation quelconque. Cependant, certaines applications utilisent des balises en distinguant les majuscules et minuscules. Nous vous recommandons d'adopter une stratégie de capitalisation standard pour votre organisation, par exemple en utilisant uniquement des noms et des valeurs de balises en minuscules. Une approche cohérente peut aider à éviter la confusion qui peut être causée par le fait d'avoir des balises qui ne diffèrent que par la façon dont elles sont mises en majuscules.

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

Rechercher des ressources dans un sous-ensemble deRégions AWS

Utilisez l'opérateur '*' joker pour faire correspondre toutes les régions d'une certaine région du monde. L'exemple suivant renvoie toutes les ressources qui se trouvent dans les régions d'Europe (UE).

```
region:eu-*
```

Rechercher des ressources mondiales

Utilisez laglobal valeur des majuscules spéciales pour leregion: filtre afin de rechercher vos ressources considérées comme globales et non associées à une région en particulier.

```
region:global
```

Rechercher des ressources d'un certain type situées dans une région spécifique

Lorsque vous utilisez plusieurs filtres, Resource Explorer évalue l'expression en combinant les préfixes avec desAND opérateurs logiques implicites. L'exemple suivant renvoie toutes les ressources de la région Asie-Pacifique (Hong Kong) quiAND sont des instances Amazon EC2.

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> En raison de l'impliciteAND, vous ne pouvez utiliser avec succès qu'un seul filtre pour un attribut qui ne peut avoir qu'une seule valeur associée à la ressource. Par exemple, une ressource ne peut faire partie que d'une seule ressourceRégion AWS. Par conséquent, la requête suivante ne renvoie aucun résultat.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Cette limitation ne s'applique pas aux filtres pour les attributs qui peuvent avoir plusieurs valeurs en même temps, tels que`tag:tag.key:`, et`tag.value:`.

Rechercher des ressources contenant un terme composé de plusieurs mots

Entourez un terme comportant plusieurs mots de guillemets doubles (") pour renvoyer uniquement les résultats dont le terme entier est dans l'ordre spécifié. Sans guillemets doubles, Resource Explorer renvoie les ressources qui correspondent aux mots individuels composant le terme. Par exemple, la requête suivante utilise les guillemets doubles pour renvoyer uniquement les ressources correspondant au terme`"west wing"`. La requête ne correspond pas aux ressources de la région`us-west-2`Région AWS (ou de toute autre région incluse`west` dans son code) ni aux ressources qui correspondent au mot « aile » sans le mot « ouest ».

```
"west wing"
```

Recherche de ressources faisant partie d'une CloudFormation pile spécifiée

Lorsque vous créez une ressource dans le cadre d'uneAWS CloudFormation pile, elle est automatiquement balisée avec le nom de la pile. L'exemple suivant renvoie toutes les ressources créées dans le cadre de la pile spécifiée.

```
tag:aws:cloudformation:stack-name=my-stack-name
```

Utilisation de la recherche unifiée dans AWS Management Console

AWS Management ConsoleIl inclut une barre de recherche en haut de chaque page de AWS console. Cette barre de recherche permet d'effectuer des recherches dans la Service AWS documentation et les rubriques du blog, et d'accéder directement aux pages de la console de AWS service. Il peut également renvoyer les ressources présentes dans votreCompte AWS, si vous activez la fonction de recherche unifiée en activant les fonctionnalités requises de l'Explorateur de ressources.

Grâce à la recherche unifiée, vos utilisateurs peuvent rechercher des ressources depuis n'importe quelle Service AWS console sans avoir à accéder d'abord à la Explorateur de ressources AWS console.

> **Tip**
>
> Lorsque vous souhaitez utiliser la barre de recherche unifiée pour rechercher spécifiquement des ressources, commencez votre recherche en tapant**`/Resources`**. Les AWS ressources sont ainsi mieux classées dans les résultats de recherche que les résultats qui ne représentent pas des ressources.

Rubriques

> **Important**
>
> La recherche unifiée insère automatiquement un opérateur de caractère générique (*) à la fin du premier mot clé de la chaîne. Cela signifie que les résultats de recherche unifiés incluent des ressources qui correspondent à n'importe quelle chaîne commençant par le mot clé spécifié.
> La recherche effectuée par la zone de texte Requête sur la page de recherche de ressources de la console Resource Explorer n'ajoute pas automatiquement de caractère générique. Vous

pouvez insérer * manuellement un caractère après n'importe quel terme de la chaîne de recherche.

Vérifier si la recherche unifiée est activée

Pour savoir si la recherche unifiée est activée dans votreCompte AWS, regardez en haut de la page Paramètres. L'Explorateur de ressources y affiche l'état actuel de chaque exigence. Les conditions requises pour la recherche unifiée pour la recherche unifiée pour la recherche unifiée :

- Vous devez activer l'Explorateur de ressources dans au moins unRégion AWS. Seules les ressources des régions dotées d'index de l'Explorateur de ressources peuvent apparaître dans les résultats de recherche unifiés.
- Vous devez créer un index agrégateur dans la région de votre choix. Les recherches effectuées dans cette région renvoient les résultats de toutes les régions enregistrées dans le compte.
- Vous devez créer une vue par défaut dans la région qui contient l'index agrégateur. Tous les utilisateurs qui ont besoin d'utiliser la recherche unifiée de ressources doivent être autorisés à utiliser cette vue par défaut.
- Les utilisateurs doivent disposer d'une politique d'autorisations AWS Identity and Access Management (IAM) attribuée à leur principal IAM qui leur accorde l'autorisation d'effectuer les `resource-explorer-2:Get*` actions, `resource-explorer-2:List*resource-explorer-2:Describe*`,`resource-explorer-2:Search`. Vous pouvez accorder ces autorisations en utilisant vos propres politiques IAM personnalisées. Ces autorisations sont déjà incluses dans les politiques AWS gérées suivantes que vous pouvez utiliser :
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

Activer la recherche unifiée

Pour permettre d'inclure les ressources de votre compte dans les résultats de recherche pour une recherche unifiée à partir de n'importe quelle AWS console, vous devez suivre les étapes suivantes :

1. Explorateur de ressources AWSActivez une ou plusieurs options Régions AWS de votre compte.
2. Enregistrez une région pour contenir l'index agrégateur.
3. Créez une vue par défaut dans la région à l'aide de l'index agrégateur.

Création de ressources de l'Explorateur de ressources avec CloudFormation

Explorateur de ressources AWSest intégré àAWS CloudFormation, un service qui vous permet de modéliser et de configurer vos AWS ressources. Cette intégration vous permet de consacrer moins de temps à la création et à la gestion de vos ressources et de votre infrastructure. Vous créerez un modèle qui décrit toutes les ressources AWS que vous souhaitez utiliser, et CloudFormation met en service et configure ces ressources. Les exemples de ressources incluent les index, les vues ou l'attribution d'une vue par défaut à unRégion AWS.

Lorsque vous utilisezCloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Resolver de manière cohérente et répétée. Il suffit de décrire vos ressources une fois, d'allouer les mêmes ressources à l'infini dans plusieurs comptes Comptes AWS et régions.

Utilisation AWS CloudFormation pour déployer Resource Explorer sur AWS Organizations

Vous pouvez l'utiliser AWS CloudFormation StackSets pour déployer Resource Explorer sur tous les comptes de votre organisation. Lorsque vous ajoutez ou créez des comptes de membres dans votre organisation, vous StackSets pouvez configurer automatiquement des index dans chacun d'entre euxRégion AWS, y compris un index agrégateur que vous spécifiez, pour chaque nouveau compte de membre. Pour des instructions, consultez Déploiement de l'explorateur de ressources sur les comptes d'une organisation.

Explorateur de ressources et CloudFormation modèles

Pour allouer et configurer des ressources pour Resolver, vous devez maîtriser les AWS CloudFormationmodèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles CloudFormation. Si JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec des modèles CloudFormation. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormationGuide de l'utilisateur.

Resolver prend en charge la création des types de ressources suivantes dans CloudFormation :

- Index : crée un index dans une région et active l'Explorateur de ressources dans cette région. Vous pouvez spécifier que l'index soit local ou qu'il s'agisse de l'index agrégateur duCompte AWS. Pour plus d'informations, consultez Activer l'explorateur de ressources Région AWS pour indexer vos ressources et Activation de la recherche interrégionale en créant un index agrégateur.

- Affichage : crée un affichage qui détermine les résultats qui peuvent apparaître lorsqu'un utilisateur effectue une recherche. Chaque opération de recherche doit spécifier une vue. Vous devez accorder aux utilisateurs l'autorisation d'utiliser les vues auxquelles vous souhaitez qu'ils accèdent. Pour plus d'informations, veuillez consulter Gestion des vues de l'explorateur de ressources pour fournir un accès à la recherche.

  > **Note**
  >
  > Vous devez créer un index dans une région avant de pouvoir créer une vue dans cette même région. Si vous créez un index et une vue dans le cadre de la même pile, utilisez l'`DependsOn`attribut de la vue, comme indiqué dans l'exemple de modèle suivant, pour vous assurer que l'index est créé en premier.

- DefaultViewAssociation— Définit la vue spécifiée comme étant la vue par défaut dans sa région. Lorsqu'un utilisateur ne spécifie pas explicitement la vue à utiliser pour une opération de recherche, Resource Explorer tente d'utiliser la vue par défaut associée à la région dans laquelle l'utilisateur effectue la recherche. Pour de plus amples informations, consultez Définition d'une vue par défaut dans unRégion AWS.

L'exemple suivant montre comment vous pouvez créer un index et une vue dans la même région, puis définir la vue comme étant la vue par défaut pour la région.

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
```

```
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
```

```
                }
            }
        }
    }
}
```

Pour en savoir plus, notamment pour obtenir des exemples de modèles JSON et YAML pour les index et les vues Resolver, consultez la Référence de type ResourceExplorer de ressource dans le Guide de l'AWS CloudFormationutilisateur.

En savoir plus sur AWS CloudFormation

Pour en savoir plus sur CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

Utilisation Amazon Q Developer in chat applications pour rechercher des ressources

Vous pouvez rechercher et découvrir des informations sur Services AWS vos AWS ressources en posant des questions en langage Amazon Q Developer in chat applications naturel. Amazon Q Developer in chat applicationsrépond aux questions relatives au service directement dans vos canaux de discussion avec de la AWS documentation pertinente et des extraits d'articles de support. Amazon Q Developer in chat applicationsutilise l'Explorateur de ressources pour rechercher et trouver des réponses à vos questions relatives aux ressources.

Pour plus d'informations, voir Qu'est-ce que c'est Amazon Q Developer in chat applications ? dans le guide de Amazon Q Developer in chat applications l'administrateur.

AWSquestions relatives aux ressources

Amazon Q Developer in chat applicationsutilise l'explorateur de ressources pour rechercher et découvrir vos ressources. Amazon Q Developer in chat applicationsaffiche ces résultats de recherche dans une liste. Cette liste présente les cinq principales ressources correspondantes et inclut la possibilité de filtrer davantage les résultats par type de ressource et par balise. Région AWS

Prérequis

Pour poser Amazon Q Developer in chat applications des questions relatives aux ressources, vous devez :

- Assurez-vous que vous disposez d'index et de vues actifs avec au moins une vue par défaut dans votreRégion AWS. Les index et les vues permettent à Resource Explorer de cataloguer et d'interroger vos ressources. Pour plus d’informations, consultez Termes et concepts pour Resource Explorer.
- Ajoutez la AWSResourceExplorerReadOnlyAccess politique à votre rôle de chaîne ou à chaque rôle d'utilisateur approprié, en fonction du schéma d'autorisation de votre chaîne.
- Vérifiez que les règles de protection de votre chaîne autorisent AWSResourceExplorerReadOnlyAccess les autorisations.

Questions fréquemment posées sur les ressources

Vous pouvez poser ces questions directement depuis vos canaux de discussion. Remplacez les mots par du texte rouge par vos propres informations.

```
@aws What services am I using in Region?
```

```
@aws What are the resources in my account with tags?
```

```
@aws What lambda functions do I have?
```

Sécurité dans Explorateur de ressources AWS

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 ceci comme la sécurité du cloud et la sécurité dans le cloud :

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

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation Explorateur de ressources AWS. Il explique comment configurer Resource Explorer pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres outils Services AWS qui vous aideront à surveiller et à sécuriser vos ressources de l'explorateur de ressources.

Table des matières

IAMPolitiques de mise à niveau vers IPv6

Explorateur de ressources AWS les clients utilisent des IAM politiques pour définir une plage d'adresses IP autorisée et empêcher les adresses IP situées en dehors de la plage configurée d'accéder à Resource ExplorerAPIs.

L'explorateur de ressources-2.*region*Le domaine .api.aws où APIs sont hébergés les explorateurs de ressources est en cours de mise à niveau pour être pris IPv6 en charge en plus de. IPv4

Les politiques de filtrage des adresses IP qui ne sont pas mises à jour pour gérer les IPv6 adresses peuvent empêcher les clients d'accéder aux ressources du API domaine Resource Explorer.

Clients concernés par la mise à niveau IPv4 de IPv6

Les clients qui utilisent le double adressage avec des politiques contenant aws : sourceIp sont concernés par cette mise à niveau. Le double adressage signifie que le réseau prend en charge à la fois IPv4 etIPv6.

Si vous utilisez le double adressage, vous devez mettre à jour vos IAM politiques actuellement configurées avec les adresses de IPv4 format afin d'inclure les adresses de IPv6 format.

Pour obtenir de l'aide concernant les problèmes d'accès, contactez Support.

> **Note**
>
> Les clients suivants ne sont pas concernés par cette mise à niveau :
>
> - Les clients connectés uniquement IPv4 aux réseaux.
> - Les clients connectés uniquement IPv6 aux réseaux.

Qu'est-ce qu'IPv6 ?

IPv6est la norme IP de prochaine génération destinée à être remplacée à termeIPv4. La version précédente utilise un schéma d'adressage 32 bits pour prendre en charge 4,3 milliards d'appareils. IPv4 IPv6utilise plutôt un adressage 128 bits pour prendre en charge environ 340 billions de billions de milliards de milliards de milliards de dollars (soit 2 appareils à la 128e puissance).

```
2001:cdba:0000:0000:0000:0000:3257:9652
```

```
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

Mettre à jour une IAM politique pour IPv6

IAMles politiques sont actuellement utilisées pour définir une plage d'adresses IP autorisée à l'aide du `aws:SourceIp` filtre.

Le double adressage prend en charge les deux IPv4 et IPV6 le trafic. Si votre réseau utilise le double adressage, vous devez vous assurer que toutes IAM les politiques utilisées pour le filtrage des adresses IP sont mises à jour pour inclure les plages d'IPv6adresses.

Par exemple, cette politique de compartiment Amazon S3 identifie les plages d'IPv4adresses autorisées `192.0.2.0.*` et `203.0.113.0.*` dans l'`Condition`élément.

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

Pour mettre à jour cette politique, l'`Condition`élément de la politique est mis à jour pour inclure les plages d'IPv6adresses `2001:DB8:1234:5678::/64` et`2001:cdba:3257:8593::/64`.

> **Note**
>
> UTILISEZ NOT REMOVE les IPv4 adresses existantes car elles sont nécessaires pour la rétrocompatibilité.

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT REMOVE existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT REMOVE existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
```

Pour plus d'informations sur la gestion des autorisations d'accès avecIAM, consultez la section Politiques gérées et politiques intégrées dans le Guide de l'AWS Identity and Access Management utilisateur.

Vérifiez que votre client peut vous aider IPv6

Clients utilisant le Resource-Explorer-2. Il est conseillé aux points de terminaison {region} .api.aws de vérifier si leurs clients peuvent accéder à d'autres Service AWS points de terminaison déjà activés. IPv6 Les étapes suivantes décrivent comment vérifier ces points de terminaison.

Cet exemple utilise Linux et la version 8.6.0 de curl et utilise les points de terminaison du service Amazon Athena qui ont activé les points de terminaison situés dans le IPv6 domaine api.aws.

> **Note**
>
> Basculez Région AWS vers la même région que celle où se trouve le client. Dans cet exemple, nous utilisons le point de `us-east-1` terminaison de l'est des États-Unis (Virginie du Nord).

1. Déterminez si le point de terminaison est résolu avec une IPv6 adresse à l'aide de la commande curl suivante.

```
dig +short AAAA athena.us-east-1.api.aws
2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
2600:1f18:e2f:4e03:4a1e:83b0:8823:4ce5
2600:1f18:e2f:4e04:34c3:6e9a:2b0d:dc79
```

2. Déterminez si le réseau client peut établir une connexion à l'IPv6aide de la commande curl suivante.

```
curl --ipv6 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
response code: 404
```

   Si une adresse IP distante a été identifiée mais que le code de réponse ne l'est pas0, une connexion réseau a été établie avec succès avec le terminal à l'aide deIPv6.

Si l'adresse IP distante est vide ou si le code de réponse l'est0, le réseau client ou le chemin réseau vers le point de IPv4 terminaison est uniquement disponible. Vous pouvez vérifier cette configuration à l'aide de la commande curl suivante.

```
curl -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 3.210.103.49
response code: 404
```

Si une adresse IP distante a été identifiée mais que le code de réponse ne l'est pas0, une connexion réseau a été établie avec succès avec le terminal à l'aide deIPv4. L'adresse IP distante doit être une IPv4 adresse car le système d'exploitation doit sélectionner le protocole valide pour le client. Si l'adresse IP distante n'est pas une IPv4 adresse, utilisez la commande suivante pour forcer l'utilisation IPv4 de curl.

```
curl --ipv4 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws
```

```
remote ip: 35.170.237.34
response code: 404
```

Gestion des identités et des accès pour Explorateur de ressources AWS

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

Rubriques

Public ciblé

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

Utilisateur du service : si vous utilisez le service Resource Explorer pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de l'Explorateur de ressources 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 l'Explorateur de ressources, consultezExplorateur de ressources AWS Permissions de dépannage.

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

IAMadministrateur : si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Resource Explorer. Pour consulter des exemples de politiques basées sur l'identité de Resource Explorer que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité Explorateur de ressources AWS

Authentification par des identités

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

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

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

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

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

Compte AWS utilisateur root

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

Utilisateurs et groupes

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

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

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

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

Rôles

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

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

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

  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations Service AWS dans le Guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui font AWS CLI des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques

déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

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

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

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

Politiques basées sur l'identité

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

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

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux

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

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

Explorateur de ressources AWS ne prend pas en charge les politiques basées sur les ressources.

Listes de contrôle d'accès (ACLs)

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

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Explorateur de ressources AWS ne supporte pasACLs.

Autres types de politique

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

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

- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

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

Comment fonctionne Resource Explorer avec IAM

Avant de gérer l'IAMaccès à Explorateur de ressources AWS, vous devez connaître les IAM fonctionnalités disponibles avec Resource Explorer. Pour obtenir une vue d'ensemble de la façon dont Resource Explorer et les autres Services AWS outils fonctionnentIAM, consultez la section Services AWS relative à leur utilisation IAM dans le guide de IAM l'utilisateur.

Rubriques

- Politiques basées sur l'identité de Resource Explorer
- Autorisation basée sur les balises Resource Explorer
- IAMRôles de Resource Explorer

Comme tout autre outil Service AWS, Resource Explorer a besoin d'autorisations pour utiliser ses opérations afin d'interagir avec vos ressources. Pour effectuer une recherche, les utilisateurs doivent être autorisés à récupérer les informations relatives à une vue et à effectuer une recherche à l'aide de cette vue. Pour créer des index ou des vues, ou pour les modifier ou pour modifier tout autre paramètre de l'explorateur de ressources, vous devez disposer d'autorisations supplémentaires.

Attribuez IAM des politiques basées sur l'identité qui accordent ces autorisations aux principaux concernésIAM. Resource Explorer fournit plusieurs politiques gérées qui prédéfinissent des ensembles communs d'autorisations. Vous pouvez les attribuer à vos IAM directeurs.

Politiques basées sur l'identité de Resource Explorer

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions autorisées ou refusées contre des ressources spécifiques et les conditions dans lesquelles ces actions sont autorisées ou refusées. Resource Explorer prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Actions

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

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

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

Les actions de stratégie dans Resource Explorer utilisent le préfixe de `resource-explorer-2` service avant l'action. Par exemple, pour autoriser quelqu'un à effectuer une recherche à l'aide d'une vue, avec l'`Search`APIopération Resource Explorer, vous incluez l'`resource-explorer-2:Search`action dans une politique attribuée à ce principal. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Resource Explorer définit son propre ensemble

d'actions décrivant les tâches que vous pouvez effectuer avec ce service. Elles s'alignent sur les API opérations de l'explorateur de ressources.

Pour préciser plusieurs actions dans une seule déclaration, séparez-les par des virgules comme l'indique l'exemple suivant.

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
]
```

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

```
"Action": "resource-explorer-2:Describe*"
```

Pour obtenir la liste des actions de l'explorateur de ressources, voir Actions définies par Explorateur de ressources AWS dans la référence d'autorisation de AWS service.

Ressources

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

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant 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": "*"
```

Vue

Le principal type de ressource de l'explorateur de ressources est la vue.

La ressource d'affichage de l'explorateur de ressources a le ARN format suivant.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

Le ARN format Resource Explorer est illustré dans l'exemple suivant.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> Le ARN formulaire pour une vue inclut un identifiant unique à la fin pour garantir que chaque vue est unique. Cela permet de garantir qu'une IAM politique accordant l'accès à une ancienne vue supprimée ne peut pas être utilisée pour autoriser accidentellement l'accès à une nouvelle vue portant le même nom que l'ancienne vue. Chaque nouvelle vue reçoit un nouvel identifiant unique à la fin afin de garantir qu'il ARNs ne sera jamais réutilisé.

Pour plus d'informations sur le format deARNs, consultez Amazon Resource Names (ARNs).

Vous utilisez des politiques IAM basées sur l'identité attribuées aux IAM principaux et vous spécifiez la vue en tant que. `Resource` Cela vous permet d'accorder l'accès à la recherche via une vue à un ensemble de principes, et l'accès via une vue complètement différente à un ensemble de principes différent.

Par exemple, pour autoriser une seule vue nommée `ProductionResourcesView` dans une déclaration de IAM politique, obtenez d'abord le nom de ressource Amazon (ARN) de la vue. Vous pouvez utiliser la page Vues de la console pour afficher les détails d'une vue ou appeler l'`ListViews`opération pour récupérer l'intégralité ARN de la vue souhaitée. Incluez-le ensuite dans une déclaration de politique, comme celle illustrée dans l'exemple suivant, qui autorise la modification de la définition d'une seule vue.

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

Pour autoriser les actions sur toutes les vues appartenant à un compte spécifique, utilisez le caractère générique (*) dans la partie correspondante duARN. L'exemple suivant accorde l'autorisation de recherche à toutes les vues d'un compte spécifique Région AWS .

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

Certaines actions de l'explorateur de ressources`CreateView`, telles que, ne sont pas effectuées sur une ressource spécifique, car, comme dans l'exemple suivant, la ressource n'existe pas encore. Dans ce cas, vous devez utiliser le caractère générique (*) pour l'ensemble de la ressourceARN.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "*"
```

Si vous spécifiez un chemin qui se termine par un caractère générique, vous pouvez limiter l'`CreateView`opération à la création de vues avec uniquement le chemin approuvé. L'exemple d'article de politique suivant montre comment autoriser le directeur à créer des vues uniquement dans le chemin`view/ProductionViews/`.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

Index

L'index est un autre type de ressource que vous pouvez utiliser pour contrôler l'accès aux fonctionnalités de l'explorateur de ressources.

La principale façon d'interagir avec l'index consiste à activer l'explorateur de ressources dans et en Région AWS créant un index dans cette région. Ensuite, vous faites presque tout le reste en interagissant avec la vue.

L'une des choses que vous pouvez faire avec l'index est de contrôler qui peut créer des vues dans chaque région.

> **Note**
>
> Une fois que vous avez créé une vue, IAM autorise toutes les autres actions de vue uniquement sur ARN la vue, et non sur l'index.

L'index contient un ARNque vous pouvez référencer dans une politique d'autorisation. Un index Resource Explorer ARN a le format suivant.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

Consultez l'exemple suivant d'index Resource ExplorerARN.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222
```

Certaines actions de l'explorateur de ressources vérifient l'authentification par rapport à plusieurs types de ressources. Par exemple, l'CreateViewopération autorise à la fois ARN l'index et la vue tels qu'ARNils seront une fois que Resource Explorer les aura créés. Pour autoriser les administrateurs à gérer le service Resource Explorer, vous pouvez `"Resource": "*"` autoriser des actions pour n'importe quelle ressource, index ou vue.

Vous pouvez également limiter un directeur à ce qu'il ne puisse travailler qu'avec des ressources spécifiques de l'explorateur de ressources. Par exemple, pour limiter les actions aux seules ressources de l'explorateur de ressources d'une région spécifiée, vous pouvez inclure un ARN modèle qui correspond à la fois à l'index et à la vue, mais qui n'appelle qu'une seule région. Dans l'exemple suivant, les ARN résultats correspondent à la fois aux index ou aux vues dans la `us-west-2` région du compte spécifié uniquement. Spécifiez la région dans le troisième champ duARN, mais utilisez un caractère générique (*) dans le dernier champ pour correspondre à n'importe quel type de ressource.

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

Pour plus d'informations, consultez la section Ressources définies par Explorateur de ressources AWS dans la référence d'autorisation de AWS service. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez la ARN section Actions définies par Explorateur de ressources AWS.

Clés de condition

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

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

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 autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

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 contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de condition que vous pouvez utiliser avec Resource Explorer, consultez la section Clés de condition correspondantes Explorateur de ressources AWS dans la référence d'autorisation de AWS service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Explorateur de ressources AWS.

Exemples

Pour consulter des exemples de politiques basées sur l'identité de Resource Explorer, consultez. Exemples de politiques basées sur l'identité Explorateur de ressources AWS

Autorisation basée sur les balises Resource Explorer

Vous pouvez associer des balises aux vues de l'explorateur de ressources ou transmettre des balises dans une demande à l'explorateur de ressources. 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 `resource-explorer-2:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Pour plus d'informations sur le balisage des ressources de l'Explorateur de ressources, consultezL'ajout d'balises aux vues. Pour utiliser l'autorisation basée sur des balises dans Resource Explorer, voirUtiliser l'autorisation basée sur des balises pour contrôler l'accès à vos vues.

IAMRôles de Resource Explorer

Un IAMrôle est un principal au sein de vous Compte AWS qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Resource Explorer

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

Resource Explorer prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés à un service permettent Services AWS d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre IAM compte et appartiennent au service. Un IAM administrateur peut consulter mais pas modifier les autorisations pour les rôles liés à un service.

Resource Explorer utilise des rôles liés à un service pour effectuer son travail. Pour plus de détails sur les rôles liés à un service Resource Explorer, consultez. Utilisation de rôles liés à un service pour Resource Explorer

Exemples de politiques basées sur l'identité Explorateur de ressources AWS

Par défaut, lesAWS Identity and Access Management entités (IAM), tels que les rôles, les groupes et les utilisateurs, ne sont pas autorisés à créer ou modifier les ressources de l'Explorateur

de ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide duAWS Management Console,AWS Command Line Interface (AWS CLI) ou deAWS l'API. Un administrateur IAM doit créer des politiques IAM autorisant les responsables à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Ensuite, l'administrateur doit attribuer ces politiques aux entités IAM qui ont besoin de ces autorisations.

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.

Pour savoir comment créer une politique IAM basée sur l'identité 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.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources de l'Explorateur de 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 :

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

multifactorielle pour une sécurité renforcée. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

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

Utilisation de la console Resource Explorer

Pour que les entités principales puissent effectuer des recherches dans laExplorateur de ressources AWS console, ils doivent disposer d'un ensemble minimum d'autorisations. Si vous ne créez pas de politique basée sur l'identité avec les autorisations minimales requises, la console de l'Explorateur de ressources ne fonctionnera pas comme prévu pour les entités principales du compte.

Vous pouvez utiliser la politiqueAWS gérée nomméeAWSResourceExplorerReadOnlyAccess pour autoriser l'utilisation de la console Resource Explorer pour effectuer des recherches à l'aide de n'importe quelle vue du compte. Pour accorder l'autorisation de rechercher avec une seule vueAutorisation de l'accès aux vues de l'Explorateur de ressources pour la recherche, consultez les exemples des deux sections suivantes.

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les principaux qui effectuent des appels uniquement à la AWS CLI ou à l'API AWS. Au lieu de cela, vous pouvez choisir de n'accorder l'accès qu'aux actions qui correspondent aux opérations d'API que les responsables doivent effectuer.

Octroi d'un accès à une vue basée sur des balises

Dans cet exemple, vous souhaitez accorder l'accès à une vue de l'ExplorateurCompte AWS de ressources dans vos deux entités principales du compte. Pour ce faire, vous devez attribuer des politiques IAM basées sur l'identité aux principaux que vous souhaitez pouvoir rechercher dans l'Explorateur de ressources. L'exemple de politique IAM suivant permet d'accéder à toute demande pour laquelle laSearch-Group balise attachée au principal appelant correspond exactement à la valeur de cette même balise attachée à la vue utilisée dans la demande.

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

```
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

Vous pouvez attribuer cette politique aux responsables IAM de votre compte. Si un utilisateur possédant la baliseSearch-Group=A tente d'effectuer une recherche à l'aide d'une vue de l'Explorateur de ressources, la vue doit également être baliséeSearch-Group=A. Si ce n'est pas le cas, l'accès est refusé au principal. La clé de condition d'étiquette Search-Group correspond à la fois à Search-group et à search-group, car les noms de clé de condition ne sont pas sensibles à la casse. Pour plus d'informations, veuillez consulter la rubrique Éléments de stratégie JSON IAM : Condition dans le Guide de l'utilisateur IAM.

> **Important**
>
> Pour voir vos ressources dans des résultats de recherche unifiés dans leAWS Management Console, les responsables doivent disposer à la fois desSearch autorisations nécessairesGetView et des autorisations pour la vue par défaut dans leRégion AWS qui contient l'index de l'agrégateur. Le moyen le plus simple d'accorder ces autorisations est de conserver l'autorisation basée sur les ressources par défaut qui était associée à la vue lorsque vous avez activé l'Explorateur de ressources à l'aide de la configuration rapide ou avancée.
>
> Dans ce scénario, vous pouvez envisager de définir la vue par défaut pour filtrer les ressources sensibles, puis de configurer des vues supplémentaires auxquelles vous accorderez un accès basé sur des balises, comme décrit dans l'exemple précédent.

Autoriser l'accès à la création d'une vue basée sur des balises

Dans cet exemple, vous souhaitez autoriser uniquement les principaux balisés de la même manière que l'index à créer des vues dans le fichierRégion AWS qui contient l'index. Pour ce faire, créez

des autorisations basées sur l'identité pour permettre aux principaux utilisateurs d'effectuer des recherches à l'aide de vues.

Vous êtes maintenant prêt à accorder l'ensemble minimum d'autorisations requis pour créer une vue. Vous pouvez ajouter les déclarations de cet exemple à la même politique d'autorisation que celle que vous utilisez pour accorder`Search` des autorisations aux responsables concernés. Les actions sont autorisées ou refusées en fonction des balises attachées aux principaux appelant les opérations et l'index auxquels la vue doit être associée. L'exemple de politique IAM suivant refuse toute demande de création d'une vue lorsque la valeur de la`Allow-Create-View` balise attachée au principal de l'appelant ne correspond pas exactement à la valeur de cette même balise attachée à l'index dans la région dans laquelle la vue est créée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

Autorisation accordée aux responsables 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 nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API 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": "*"
        }
    ]
}
```

Exemples de politiques de contrôle des services pour AWS Organizations et Resource Explorer

Explorateur de ressources AWS prend en charge les politiques de contrôle des services (SCP). Les SCP sont des politiques que vous attachez aux éléments d'une organisation pour gérer les autorisations au sein de cette organisation. Un SCP s'applique Comptes AWS à tous les membres d'une organisation sous l'élément auquel vous attachez le SCP. Les politiques de contrôle des services (SCP) offrent un contrôle central sur les autorisations maximales disponibles pour tous les comptes de votre organisation. Ils peuvent vous aider à garantir le respect Comptes AWS des directives de contrôle d'accès de votre organisation. Pour plus d'informations, consultez la section Politiques de contrôle de service du Guide de l'utilisateur AWS Organizations .

Prérequis

Procédez comme suit pour utiliser les SCP :

- Activez toutes les fonctions de votre organisation. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations .
- Activez les SCP au sein de votre organisation. Pour plus d'informations, voir la rubrique Activation et désactivation des types des politiques du Guide de l'utilisateur AWS Organizations .
- Créez les SCP dont vous avez besoin. Pour plus d'informations sur la création de SCP, voir Création et mise à jour de SCP dans le guide de l'AWS Organizations utilisateur.

Exemples de politiques de contrôle des services

L'exemple suivant montre comment utiliser le contrôle d'accès basé sur les attributs (ABAC) pour contrôler l'accès aux opérations administratives de Resource Explorer. Cet exemple de politique refuse l'accès à toutes les opérations de Resource Explorer, à l'exception des deux autorisations requises pour effectuer une recherche `resource-explorer-2:Search` et`resource-explorer-2:GetView`, sauf si le principal IAM qui fait la demande est étiqueté`ResourceExplorerAdmin=TRUE`. Pour une discussion plus complète sur l'utilisation d'ABAC avec Resource Explorer, voirUtiliser l'autorisation basée sur des balises pour contrôler l'accès à vos vues.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
```

```
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
   ]
}
```

AWS politiques gérées pour Explorateur de ressources AWS

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

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

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

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

Politiques générales AWS gérées qui incluent les autorisations de l'explorateur de ressources

- AdministratorAccess— Accorde un accès complet aux ressources Services AWS et aux ressources.
- ReadOnlyAccès : accorde un accès en lecture seule aux ressources Services AWS et à leurs ressources.

- ViewOnlyAccès : autorise l'affichage des ressources et des métadonnées de base pour Services AWS.

> **Note**
>
> Les `Get*` autorisations de l'explorateur de ressources incluses dans la `ViewOnlyAccess` politique fonctionnent comme `List` des autorisations, bien qu'elles ne renvoient qu'une seule valeur, car une région ne peut contenir qu'un seul index et une seule vue par défaut.

AWS politiques gérées pour Resource Explorer

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS politique gérée : AWSResourceExplorerFullAccess

Vous pouvez attribuer la `AWSResourceExplorerFullAccess` politique à vos identités IAM.

Cette politique accorde des autorisations qui permettent un contrôle administratif total du service Resource Explorer. Vous pouvez effectuer toutes les tâches liées à l'activation et à la gestion de l'Explorateur de ressources Régions AWS dans votre compte.

Détails de l'autorisation

Cette politique inclut des autorisations qui autorisent toutes les actions pour Resource Explorer, y compris l'activation et la désactivation de Resource Explorer dans Régions AWS, la création ou la suppression d'un index agrégateur pour le compte, la création, la mise à jour et la suppression de vues, ainsi que la recherche. Cette politique inclut également les autorisations qui ne font pas partie de Resource Explorer :

- `ec2:DescribeRegions`— permet à Resource Explorer d'accéder aux informations relatives aux régions de votre compte.
- `ram:ListResources`— permet à Resource Explorer de répertorier les partages de ressources dont font partie les ressources.
- `ram:GetResourceShares`— permet à Resource Explorer d'identifier les informations relatives aux partages de ressources que vous possédez ou qui sont partagés avec vous.

- `iam:CreateServiceLinkedRole`— permet à Resource Explorer de créer le rôle lié au service requis lorsque vous activez Resource Explorer en créant le premier index.
- `organizations:DescribeOrganization`— permet à Resource Explorer d'accéder aux informations relatives à votre organisation.

Pour consulter la dernière version de cette politique AWS gérée, consultez `AWSResourceExplorerFullAccess` le Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSResourceExplorerReadOnlyAccess

Vous pouvez attribuer la `AWSResourceExplorerReadOnlyAccess` politique à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs d'accéder à la recherche de base pour découvrir leurs ressources.

Détails de l'autorisation

Cette politique inclut des autorisations qui permettent aux utilisateurs d'exécuter l'explorateur `Get*` de ressources et des `Search` opérations permettant d'afficher des informations sur les composants et les paramètres de configuration de l'explorateur de ressources, mais n'autorise pas les utilisateurs à les modifier. `List*` Les utilisateurs peuvent également effectuer une recherche. Cette politique inclut également deux autorisations qui ne font pas partie de Resource Explorer :

- `ec2:DescribeRegions`— permet à Resource Explorer d'accéder aux informations relatives aux régions de votre compte.
- `ram:ListResources`— permet à Resource Explorer de répertorier les partages de ressources dont font partie les ressources.
- `ram:GetResourceShares`— permet à Resource Explorer d'identifier les informations relatives aux partages de ressources que vous possédez ou qui sont partagés avec vous.
- `organizations:DescribeOrganization`— permet à Resource Explorer d'accéder aux informations relatives à votre organisation.

Pour consulter la dernière version de cette politique AWS gérée, consultez `AWSResourceExplorerReadOnlyAccess` le Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSResourceExplorerServiceRolePolicy

Vous ne pouvez vous associer `AWSResourceExplorerServiceRolePolicy` à aucune entité IAM vous-même. Cette politique ne peut être attachée qu'à un rôle lié à un service qui permet à Resource Explorer d'effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour Resource Explorer.

Cette politique accorde les autorisations nécessaires à Resource Explorer pour récupérer des informations sur vos ressources. Resource Explorer renseigne les index qu'il gère dans chacun des index Région AWS que vous enregistrez.

Pour consulter la dernière version de cette politique AWS gérée, consultez `AWSResourceExplorerServiceRolePolicy` la console IAM.

AWS politique gérée : AWSResourceExplorerOrganizationsAccess

Vous pouvez attribuer `AWSResourceExplorerOrganizationsAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives à Resource Explorer et accorde des autorisations en lecture seule à d'autres personnes pour prendre Services AWS en charge cet accès. L' AWS Organizations administrateur a besoin de ces autorisations pour configurer et gérer la recherche multi-comptes dans la console.

Détails de l'autorisation

Cette politique inclut des autorisations qui permettent aux administrateurs de configurer la recherche multi-comptes pour l'organisation :

- `ec2:DescribeRegions`— Permet à Resource Explorer d'accéder aux informations relatives aux régions de votre compte.
- `ram:ListResources`— Permet à Resource Explorer de répertorier les partages de ressources dont font partie les ressources.
- `ram:GetResourceShares`— Permet à l'explorateur de ressources d'identifier les informations relatives aux partages de ressources que vous possédez ou qui sont partagés avec vous.
- `organizations:ListAccounts`— Permet à Resource Explorer d'identifier les comptes au sein d'une organisation.
- `organizations:ListRoots`— Permet à Resource Explorer d'identifier les comptes racine au sein d'une organisation.

- `organizations:ListOrganizationalUnitsForParent`— Permet à Resource Explorer d'identifier les unités organisationnelles (UO) d'une unité organisationnelle parent ou d'une racine.
- `organizations:ListAccountsForParent`— Permet à Resource Explorer d'identifier les comptes d'une organisation qui sont contenus par la racine cible spécifiée ou par une unité d'organisation.
- `organizations:ListDelegatedAdministrators`— Permet à Resource Explorer d'identifier les AWS comptes désignés comme administrateurs délégués dans cette organisation.
- `organizations:ListAWSServiceAccessForOrganization`— Permet à Resource Explorer d'identifier une liste de ceux Services AWS qui sont autorisés à s'intégrer à votre organisation.
- `organizations:DescribeOrganization`— Permet à Resource Explorer de récupérer des informations sur l'organisation à laquelle appartient le compte de l'utilisateur.
- `organizations:EnableAWSServiceAccess`— Permet à Resource Explorer d'activer l'intégration d'un Service AWS (le service spécifié par`ServicePrincipal`) avec AWS Organizations.
- `organizations:DisableAWSServiceAccess`— Permet à Resource Explorer de désactiver l'intégration d'un Service AWS (le service spécifié par ServicePrincipal) avec AWS Organizations.
- `organizations:RegisterDelegatedAdministrator`— Permet à Resource Explorer d'activer le compte de membre spécifié pour administrer les fonctionnalités du AWS service spécifié de l'organisation.
- `organizations:DeregisterDelegatedAdministrator`— Permet à Resource Explorer de supprimer le membre spécifié Compte AWS en tant qu'administrateur délégué pour le membre spécifié Service AWS.
- `iam:GetRole`— Permet à Resource Explorer de récupérer des informations sur le rôle spécifié, notamment le chemin, le GUID, l'ARN du rôle, ainsi que la politique de confiance du rôle qui accorde l'autorisation d'assumer le rôle.
- `iam:CreateServiceLinkedRole`— Permet à Resource Explorer de créer le rôle lié au service requis lorsque vous activez Resource Explorer en créant le premier index.

Pour consulter la dernière version de cette politique AWS gérée, consultez `AWSResourceExplorerOrganizationsAccess` la console IAM.

Mises à jour des politiques AWS gérées par Resource Explorer

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour Resource Explorer depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes

automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents de l'Explorateur de ressources.

Modification	Description	Date
AWSResourceExplorerServiceRolePolicy- Autorisations de politique mises à jour pour afficher des types de ressources supplémentaires	Resource Explorer a ajouté des autorisations à la politique de rôle liée au service AWSResourceExplorerServiceRolePolicy qui permet à Resource Explorer d'afficher des types de ressources supplémentaires : • apprunner:ListVpcConnectors • backup:ListReportPlans • emr-serverless:ListApplications • events:ListEventBuses • geo:ListPlaceIndexes • geo:ListTrackers • greengrass:ListComponents • greengrass:ListComponentVersions • iot:ListRoleAliases • iottwinmaker:ListComponentTypes • iottwinmaker:ListEntities	12 décembre 2023

Modification	Description	Date
	• iottwinmaker:ListScenes • kafka:ListConfigurations • kms:ListKeys • kinesisanalytics:ListApplications • lex:ListBots • lex:ListBotAliases • mediapackage-vod:ListPackagingConfigurations • mediapackage-vod:ListPackagingGroups • mq:ListBrokers • personalize:ListDatasetGroups • personalize:ListDatasets • personalize:ListSchemas • route53:ListHealthChecks • route53:ListHostedZones • secretsmanager:ListSecrets	

Modification	Description	Date
Nouvelle politique gérée par	Resource Explorer a ajouté la politique AWS gérée suivante : • AWSResourceExplorerOrganizationsAccess	14 novembre 2023
Mise à jour des stratégies gérées par	Resource Explorer a mis à jour les politiques AWS gérées suivantes pour prendre en charge la recherche multi-comptes : • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	14 novembre 2023

Modification	Description	Date
AWSResourceExplorerServiceRolePolicy— Politique mise à jour pour prendre en charge la recherche multi-comptes auprès des Organizations	Resource Explorer a ajouté des autorisations à la politique des rôles liés au service AWSResourceExplorerServiceRolePolicy qui permet à Resource Explorer de prendre en charge la recherche multi-comptes auprès des Organizations : • `organizations:ListAWSServiceAccessForOrganization` • `organizations:DescribeAccount` • `organizations:DescribeOrganization` • `organizations:ListAccounts` • `organizations:ListDelegatedAdministrators`	14 novembre 2023

Modification	Description	Date
AWSResourceExplorerServiceRolePolicy— Politique mise à jour pour prendre en charge des types de ressources supplémentaires	Resource Explorer a ajouté des autorisations à la politique de rôle liée au service AWSResourceExplorerServiceRolePolicy qui permet au service d'indexer les types de ressources suivants : • analyseur d'accès : analyseur • acmpca : autorité de certification • amplifier : application • amplifier : environnement principal • amplifier : branche • amplifier : association de domaines • amplifyuibuilder:composant • amplifyuibuilder : thème • intégrations d'applications : intégration d'événements • apprunner:service • appstream : appblock • appstream : application • Appstream : flotte • appstream : générateur d'images • flux d'applications : stack • appsync : graphqlapi	17 octobre 2023

Modification	Description	Date
	• espace de noms aps:ruleg roups • aps:espace de travail • apigateway:restapi • apigateway:déploiement • athena : catalogue de données • athena : groupe de travail • autoscaling:groupe de mise à l'échelle automatique • sauvegarde : plan de sauvegarde • lot : environnement informati que • lot : file d'attente de tâches • lot : politique de planification • formation du cloud : pile • formation du cloud : stackset • cloudfront : configuration du chiffrement au niveau du champ • cloudfront : profil de chiffrement au niveau du champ • cloudfront : contrôle d'accès à l'origine • cloudtrail : sentier • codeartefact : domaine • artefact de code : référentiel • codecommit:dépôt	

Modification	Description	Date
	• codeguru profiler : groupe de profilage • connexions codestar : connexion • databrew:ensemble de données • databre:recette • databrew:ensemble de règles • détective:graph • services d'annuaire : annuaire • ec2 : passerelle Carrier • ec2 : point de terminaison d'accès vérifié • ec2 : groupe d'accès vérifié • ec2 : instance à accès vérifié • ec2 : fournisseur de confiance d'accès vérifié • ecr : référentiel • elasticache : groupe de sécurité du cache • système de fichiers élastique : point d'accès • événements:règle • évidemment : expérience • évidemment : fonctionnalité • évidemment : lancement • évidemment : projet • finspace : environnement	

Modification	Description	Date
	• firehose : flux de livraison • simulateur d'injection par défaut : modèle d'expérience • prévision : groupe de jeux de données • prévision:jeu de données • détecteur de fraude : détecteur • détecteur de fraude : type d'entité • détecteur de fraude : type d'événement • détecteur de fraude : étiquette • détecteur de fraude : résultat • détecteur de fraude : variable • gamelift : alias • accélérateur global : accélérateur • accélérateur global : groupe de points de terminaison • accélérateur global : écouteur • colle : base de données • colle : job • colle : table • colle : déclencheur • herbe verte : groupe	

Modification	Description	Date
	• Healthlake : magasin de données FHIR • iam : appareil mfa virtuel • générateur d'images : version de construction du composant • générateur d'images : composant • générateur d'images : recette de conteneur • générateur d'images : configuration de distribution • générateur d'image : version de construction d'image • générateur d'images : pipeline d'images • générateur d'images : recette d'image • générateur d'image:image • générateur d'images : configuration de l'infrast ructure • IoT : autorisateur • IoT : modèle de travail • IoT : mesures d'atténuation • IoT : modèle de provision nement • IoT : profil de sécurité • IoT : chose • IoT : destination des règles du sujet	

Modification	Description	Date
	• IoT Analytics : canal • analyse de l'IoT : ensemble de données • IoT Analytics : banque de données • analyse de l'IoT : pipeline • IoT Events : modèle d'alarme • événements IoT : modèle de détecteur • événements IoT : entrée • IoT sur le site : modèle d'actifs • IoT au niveau du site : actif • IoT au niveau du site : passerelle • iottwinmaker : espace de travail • ivs : canal • ivs : Streamkey • Kafka : cluster • Kinesis Video:stream • lambda : alias • lambda : version de couche • lambda : couche • lookoutmetrics : alerte • lookoutvision:projet • package multimédia : canal • package multimédia : point de terminaison d'origine	

Modification	Description	Date
	• mediatailor : configuration de lecture • memorydb : acl • memorydb:cluster • memorydb : groupe de paramètres • memorydb : utilisateur • ciblage mobile : application • ciblage mobile : segment • ciblage mobile : modèle • pare-feu réseau : politique de pare-feu • pare-feu réseau : pare-feu • gestionnaire de réseau : réseau mondial • gestionnaire de réseau : appareil • gestionnaire de réseau : lien • gestionnaire de réseau : pièce jointe • gestionnaire de réseau : réseau principal • panorama : package • qldb : journal kinesis streams pour ledger • qldb : ledger • rds : déploiement de bluegreen • espaces de refactorisation : application	

Modification	Description	Date
	• espaces de refactorisation : environnement • espaces de refactorisation : itinéraire • espaces de refactorisation : service • reconnaissance : projet • hub de résilience : application • hub de résilience : politique de résilience • groupes de ressources:groupe • route 53 : groupe de récupération • route 53 : ensemble de ressources • route 53 : domaine de pare-feu • route 53 : groupe de règles de pare-feu • route 53 : point de terminaison du résolveur • route 53 : règle du résolveur • sagemaker : modèle • sagemaker:instance de bloc-notes • signataire : profil de signature • incidents SSM : plan de réponse	

Modification	Description	Date
	• ssm : entrée d'inventaire • ssm : synchronisation des données de ressources • états : activité • flux temporel : base de données • sagesse : assistant • sagesse : association assistante • sagesse : base de connaissances	

Modification	Description	Date
AWSResourceExplorerServiceRolePolicy— Politique mise à jour pour prendre en charge des types de ressources supplémentaires	Resource Explorer a ajouté des autorisations à la politique de rôle liée au service AWSResourceExplorerServiceRolePolicy qui permet au service d'indexer les types de ressources suivants : • codebuild:projet • code pipeline : pipeline • cognito : identitypool • cognito : pool d'utilisateurs • ecr : référentiel • efs:système de fichiers • tige de haricot élastique : application • Elasticbeanstalk : version de l'application • tige de haricot élastique : environnement • IoT : politique • IoT : règle thématique • fonctions d'étape : machine à états • s3 : seau	1er août 2023

Modification	Description	Date
AWSResourceExplorerServiceRolePolicy— Politique mise à jour pour prendre en charge des types de ressources supplémentaires	Resource Explorer a ajouté des autorisations à la politique de rôle liée au service AWSResourceExplorerServiceRolePolicy qui permet au service d'indexer les types de ressources suivants : • elasticache:cluster • elasticache : groupe de réplication global • elasticache : groupe de paramètres • elasticache : groupe de réplication • elasticache : instance réservée • Elasticache : instantané • elasticache : groupe de sous-réseaux • elasticache:utilisateur • elasticache : groupe d'utilisateurs • lambda : configuration de signature de code • lambda : mappage de la source des événements • sqs:file d'attente	7 mars 2023

Modification	Description	Date
Nouvelles politiques gérées	Resource Explorer a ajouté les politiques AWS gérées suivantes : • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	7 novembre 2022
Resource Explorer a commencé à suivre les modifications	Resource Explorer a commencé à suivre les modifications apportées AWS à ses politiques gérées.	7 novembre 2022

Utilisation de rôles liés à un service pour Resource Explorer

Explorateur de ressources AWS utilise AWS Identity and Access Management (IAM) des rôles liés à un service. Un rôle lié à un service est un type unique de IAM rôle directement lié à Resource Explorer. Les rôles liés au service sont prédéfinis par Resource Explorer 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 de l'Explorateur de ressources, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. L'explorateur de ressources définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul l'explorateur de ressources peut assumer ses rôles. Les autorisations définies incluent à la fois la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attribuée à aucune autre IAM entité.

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

Autorisations de rôle liées à un service pour Resource Explorer

L'explorateur de ressources utilise le rôle lié au service nommé. `AWSServiceRoleForResourceExplorer` Ce rôle autorise le service Resource Explorer à consulter en votre nom les ressources et les AWS CloudTrail événements qui Compte AWS s'y trouvent et à indexer ces ressources pour faciliter la recherche.

Le rôle `AWSServiceRoleForResourceExplorer` lié au service ne fait confiance qu'au service dont le principal de service est le suivant pour assumer le rôle :

- `resource-explorer-2.amazonaws.com`

La politique d'autorisation de rôle nommée AWSResourceExplorerServiceRolePolicy autorise l'accès en lecture seule à Resource Explorer pour récupérer les noms des ressources et les propriétés des ressources prises en charge AWS . Pour voir les services et les ressources pris en charge par Resource Explorer, voir Types de ressources que vous pouvez rechercher avec Resource Explorer. Pour obtenir la liste complète de toutes les actions que ce rôle peut effectuer, vous pouvez consulter la `AWSResourceExplorerServiceRolePolicy` politique dans la IAM console.

Un principal est une IAM entité telle qu'un utilisateur, un groupe ou un rôle. Si vous laissez Resource Explorer créer le rôle lié au service pour vous lorsqu'il crée l'index dans la première région du compte, le principal exécutant la tâche n'a besoin que des autorisations requises pour créer l'index Resource Explorer. Pour créer le rôle lié à un service manuellement à l'aide deIAM, le principal exécutant la tâche doit être autorisé à créer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

Création d'un rôle lié à un service pour Resource Explorer

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez l'explorateur de ressources dans le AWS Management Console ou que vous l'exécutez CreateIndexdans le premier Région AWS dans votre compte à l'aide du AWS CLI ou un AWS API, l'explorateur de ressources crée le rôle lié au service pour vous.

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 vous RegisterResourceExplorertrouvez dans la première région de votre compte, Resource Explorer crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Resource Explorer

L'Explorateur de ressources ne vous permet pas de modifier le rôle `AWSServiceRoleForResourceExplorer` 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 au rôle. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Supprimer un rôle lié à un service pour Resource Explorer

Vous pouvez utiliser la IAM console AWS CLI, le ou le AWS API pour supprimer manuellement le rôle lié au service. Pour ce faire, vous devez d'abord supprimer les index de l'explorateur de ressources de tous Région AWS les index de votre compte, puis supprimer manuellement le rôle lié à un service.

> **Note**
>
> Si le service Resource Explorer utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression échoue. Dans ce cas, assurez-vous que tous les index de toutes les régions sont supprimés, puis attendez quelques minutes et recommencez l'opération.

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

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

Régions prises en charge pour les rôles liés au service Resource Explorer

Resource Explorer prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour de plus amples informations, veuillez consulter Points de terminaison Service AWS dans le Référence générale d'Amazon Web Services.

Explorateur de ressources AWS Permissions de dépannage

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

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Resource Explorer
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon explorateur de ressources

Je ne suis pas autorisé à effectuer une action dans Resource Explorer

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 les informations d'identification que vous avez utilisées pour tenter cette opération.

Par exemple, l'erreur suivante se produit lorsqu'une personne assumant le rôle IAM `MyExampleRole` essaie d'utiliser la console pour afficher les détails d'une vue sans y être `resource-explorer-2:GetView` autorisée.

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Dans ce cas, la personne utilisant le rôle doit demander à l'administrateur de mettre à jour les politiques d'autorisation du rôle afin d'autoriser l'accès à la vue à l'aide de l'`resource-explorer-2:GetView`action.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon explorateur de ressources

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 Resource Explorer prend en charge ces fonctionnalités, consultezComment fonctionne Resource Explorer 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 en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Protection des données dans Explorateur de ressources AWS

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans Explorateur de ressources AWS. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

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

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.

- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Resource Explorer ou autre Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement au repos

Les données stockées par Resource Explorer incluent la liste indexée des ressources et des ressources associées utilisées par le client, ainsi ARNs que les vues permettant d'y accéder.

Ces données sont chiffrées lorsqu'elles sont au repos en utilisant AWS Key Management Service (AWS KMS) des clés de chiffrement symétriques qui implémentent la norme de chiffrement avancée (AES) en mode compteur Galois (GCM) avec des clés de 256 bits (AES-256-). GCM

Chiffrement en transit

Les demandes des clients et toutes les données associées sont cryptées en transit à l'aide de Transport Later Security (TLS) 1.2 ou version ultérieure. Tous les points de terminaison Resource Explorer prennent en HTTPS charge le chiffrement des données en transit. Pour obtenir la liste des points de terminaison du service Resource Explorer, consultez la section Explorateur de ressources AWS Points de terminaison et quotas dans le. Références générales AWS

Validation de la conformité pour Explorateur de ressources AWS

Pour savoir si un Service AWS est inclus dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section Portée par programme de conformité. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact le Guide de AWS Artifact l'utilisateur.

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

- Guides démarrage rapide de la sécurité et de la conformité. Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- 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.

- Ressources de conformité AWS : cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub – Ce service AWS fournit une vue complète de votre état de sécurité au sein d'AWS qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.

Résilience dans Explorateur de ressources AWS

L'infrastructureAWS mondiale d'repose surRégions AWS des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

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

Sécurité de l'infrastructure dans Explorateur de ressources AWS

En tant que service géré, Explorateur de ressources AWS 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 les API appels AWS publiés pour accéder à Resource Explorer via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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

Pour plus d'informations sur les procédures de sécurité du réseau AWS mondial, consultez le livre blanc Amazon Web Services : présentation des processus de sécurité.

Surveillance des Explorateur de ressources AWS

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances deExplorateur de ressources AWS et de vos autresAWS solutions. AWSfournit les outils de surveillance suivants pour surveiller Resource Explorer, signaler les problèmes et prendre des mesures automatiques le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés créés par votre Compte AWS ou au nom de celui-ci et livre les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour plus d'informations, veuillez consulter Journalisation des appels d'API Explorateur de ressources AWS avec AWS CloudTrail et le Guide de l'utilisateur AWS CloudTrail.

Journalisation des appels d'API Explorateur de ressources AWS avec AWS CloudTrail

Explorateur de ressources AWSest intégré àAWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un explorateurService AWS de ressources. CloudTrail capture les appels d'API pour l'Explorateur de ressources en tant qu'événements. Les appels capturés incluent les appels de la console Resource Explorer et les appels de code vers les opérations d'API de l'API Resource.

Si vous créez un journal d'activité, vous pouvez activer la livraison continue des CloudTrail événements dans un compartiment Amazon S3, y compris les événements pour Resource Explorateur de ressources. Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Resource Explorateur, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur de la demande, la date de la demande, ainsi que d'autres détails.

Pour en savoir plus CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

Informations sur l'Explorateur de ressources dans CloudTrail

CloudTrail est activé dans votreCompte AWS lors de la création de ce dernier. Lorsqu'une activité se produit dans Explorateur de ressources, cette activité est enregistrée dans un CloudTrail événement avec d'autresService AWS événements dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, consultez Affichage des événements avec l'historique des CloudTrail événements.

> **Important**
>
> Vous pouvez trouver tous les événements de Resource Explorer en recherchant Event source = resource-explorer-2.amazonaws.com

Pour obtenir un enregistrement continu des événements dans votreCompte AWS, créez un journal de suivi. Un journal CloudTrail de suivi permet la remise de fichiers journaux vers un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autresServices AWS pour analyser plus en profondeur les données d'événement collectées dans les CloudTrail journaux et agir sur celles-ci. Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrailGuide de l'utilisateur :

- Création d'un journal d'activité pour votre Compte AWS
- AWSintégrations de services avec CloudTrail Logs
- Configuration des notifications Amazon SNS Spour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions
- Réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions de l'explorateur de ressources sont consignées CloudTrail et documentées dans la Référence desExplorateur de ressources AWS API. Par exemple, les appels aux`UpdateIndex` actions`CreateIndex``DeleteIndex`, et génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initiée la demande.

- Compte AWSinformations d'identification root
- Informations d'identification de sécurité temporaires correspondant à un rôle ou un utilisateur fédéré AWS Identity and Access Management (IAM).
- Informations d'identification de sécurité à long terme d'un utilisateur IAM.
- Autre service AWS.

> **Important**
>
> Pour des raisons de sécurité`TagsFilters`, toutes les`QueryString` valeurs et les valeurs ont été supprimées des entrées CloudTrail du journal.

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

Présentation des entrées des entrées des entrées des entrées des entrées des entrées des entrées

Un journal de suivi est une configuration qui permet la remise d'événements sous forme de fichiers journaux vers un compartiment Amazon S3 que vous spécifiez. CloudTrail les entrées des entrées de journal peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail Les entrées des appels d'API publics

Rubriques

- CreateIndex
- DeleteIndex
- UpdateIndexType
- Search
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateIndex`action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
```

```
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


DeleteIndex

L'exemple suivant montre une entrée de entrée de entrée CloudTrail longue qui illustre l'`DeleteIndex`action.

> **Note**
>
> Cette action supprime également de manière asynchrone toutes les vues du compte dans cette région, ce qui entraîne un`DeleteView` événement pour chaque vue supprimée.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

UpdateIndexType

L'exemple suivant montre une entrée de CloudTrail journal qui décrit l'`UpdateIndexType`action permettant de promouvoir un index du type`LOCAL` à`AGGREGATOR`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Search

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`Search`action.

> **Note**
>
> Pour des raisons de sécurité, toutes les références à`TagFilters`, et tous les`QueryString` paramètres sont supprimés dans les entrées CloudTrail du journal.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-03T16:50:11Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
```

```
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

CreateView

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateView`action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


DeleteView

L'exemple suivant montre une entrée de CloudTrail journal qui montre l'événement qui peut se produire lorsque l'`DeleteView`action démarre automatiquement en raison d'une`DeleteIndex` opération effectuée dans celle-ciRégion AWS.

> **Note**
>
> Si la vue supprimée est la vue par défaut pour la région, cette action dissocie également la vue de manière asynchrone en tant que vue par défaut. Cela produit un`DisassociateDefaultView` événement.


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
```

```
}
```

DisassociateDefaultView

L'exemple suivant montre une entrée de CloudTrail journal qui montre l'événement qui peut se produire lorsque l'`DisassociateDefaultView`action démarre automatiquement en raison d'une`DeleteView` opération sur la vue par défaut actuelle.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Dépannage des ressources

Si vous rencontrez des problèmes lors de l'utilisation de l'Explorateur de ressources, reportez-vous aux rubriques de cette section. Consultez égalementExplorateur de ressources AWS Permissions de dépannage la section Sécurité de ce guide.

Rubriques

- Problèmes généraux(cette page)
- Résolution des problèmes d'installation et de configuration de Resource Explorer
- Résolution des problèmes de recherche dans Resource Explorer

Problèmes généraux

Rubriques

- J'ai reçu un lien vers l'Explorateur de ressources, mais lorsque je l'ouvre, la console ne montre qu'une erreur.
- Pourquoi la recherche unifiée dans la console provoque-t-elle des erreurs « accès refusé » dans mes CloudTrail journaux ?

J'ai reçu un lien vers l'Explorateur de ressources, mais lorsque je l'ouvre, la console ne montre qu'une erreur.

Certains outils tiers génèrent des URL de liens vers des pages dans l'Explorateur de ressources. Dans certains cas, ces URL n'incluent pas le paramètre qui dirige la console vers une URL spécifiqueRégion AWS. Si vous ouvrez un tel lien, la console Resource Explorer n'est pas informée de la région à utiliser et utilise par défaut la dernière région à laquelle l'utilisateur s'est connecté. Si l'utilisateur n'est pas autorisé à accéder à l'Explorateur de ressources dans cette région, la console essaie d'utiliser la région USA Est (Virginie du Nord`us-east-1`) () ou USA Ouest (Oregon) (`us-west-2`) si la console n'y parvient pas`us-east-1`.

Si l'utilisateur n'est pas autorisé à accéder à l'index dans l'une de ces régions, la console Resource Explorer renvoie une erreur.

Vous pouvez éviter ce problème en vous assurant que tous les utilisateurs disposent des autorisations suivantes :

- `ListIndexes`— aucune ressource spécifique ; utilisation*.
- `GetIndex`pour l'ARN de chaque index créé dans le compte. Pour éviter d'avoir à rétablir les politiques d'autorisation si vous supprimez et recréez un index, nous vous recommandons d'utiliser*.

La politique minimale pour y parvenir peut ressembler à l'exemple suivant :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

Vous pouvez également envisager d'associer l'autorisationAWS gérée`AWSResourceExplorerReadOnlyAccess` à tous les utilisateurs qui doivent utiliser l'Explorateur de ressources. Cela accorde les autorisations requises, ainsi que les autorisations nécessaires pour voir les vues disponibles dans la région et effectuer des recherches à l'aide de ces vues.

Pourquoi la recherche unifiée dans la console provoque-t-elle des erreurs « accès refusé » dans mes CloudTrail journaux ?

La recherche unifiée dans leAWS Management Console permet aux principaux de rechercher à partir de n'importe quelle page duAWS Management Console. Les résultats peuvent inclure des ressources provenant du compte du principal si l'Explorateur de ressources est activé et configuré pour prendre en charge la recherche unifiée. Chaque fois que vous commencez à taper dans la barre de recherche unifiée, la recherche unifiée tente d'appeler`resource-explorer-2:ListIndexes` l'opération pour vérifier si elle peut inclure des ressources du compte de l'utilisateur dans les résultats.

La recherche unifiée utilise les autorisations de l'utilisateur actuellement connecté pour effectuer cette vérification. Si cet utilisateur n'est pas autorisé à appeler`resource-explorer-2:ListIndexes`

dans une politique d'autorisation associéeAWS Identity and Access Management (IAM), la vérification échoue. Cet échec est ajouté en tant qu'`Access denied`entrée dans vos CloudTrail journaux.

Cette entrée de CloudTrail journal possède les caractéristiques suivantes :

- Source de l'événement :`resource-explorer-2.amazonaws.com`
- Nom de l'événement :`ListIndexes`
- Code d'erreur :`403` (Accès refusé)

Les politiquesAWS gérées suivantes incluent l'autorisation d'appeler`resource-explorer-2:ListIndexes`. Si vous attribuez l'une de ces règles au principal ou à toute autre politique incluant cette autorisation, cette erreur ne se produit pas :

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

Résolution des problèmes d'installation et de configuration de Resource Explorer

Utilisez ces informations pour identifier et résoudre les problèmes qui peuvent survenir lors de l'installation ou de la configuration initialeExplorateur de ressources AWS.

Rubriques

- reçois message « Accès refusé » lorsque j'effectue demande à
- Je reçois un message « Accès refusé » lorsque j'effectue une demande avec des informations d'identification de sécurité temporaires

reçois message « Accès refusé » lorsque j'effectue demande à

- Vérifiez que vous avez les autorisations nécessaires pour appeler l'action et la ressource que vous avez demandées. Un administrateur peut accorder des autorisations en attribuant une politique d'autorisationAWS Identity and Access Management (IAM) à votre principal IAM, telle qu'un rôle, un groupe ou un utilisateur.

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.

  La politique doit autoriser les`Action` données demandées`Resource` auxquelles vous souhaitez accéder.

  Si les instructions de politique qui accordent ces autorisations incluent des conditions, comme time-of-day des restrictions quant vous envoyez la demande. Pour plus d'informations sur l'affichage ou la modification de politiques pour un principal IAM, consultez Gestion de politiques IAM dans le Guide de l'utilisateur IAM.

- Si vous signez des demandes d'API manuellement (sans utiliser les AWSkits SDK), vérifiez que vous avez correctement signé la demande.

Je reçois un message « Accès refusé » lorsque j'effectue une demande avec des informations d'identification de sécurité temporaires

- Vérifiez que le principal IAM que vous utilisez pour effectuer la demande dispose des autorisations appropriées. Les autorisations affectées aux informations d'identification de sécurité temporaires proviennent d'un principal défini IAM. Elles sont donc limitées à celles accordées au principal. Pour de plus amples informations sur la définition des autorisations des informations d'identification de sécurité temporaires des informations d'identification de sécurité temporaires du Guide de l'utilisateur IAM.

- Vérifiez que vos demandes sont signées correctement et que la demande est correctement formée. Pour plus de détails, consultez la documentation de la boîte à outils correspondant au SDK que vous avez choisi ou utilisez des informations d'identification temporaires avecAWS des ressources dans le guide de l'utilisateur IAM.
- Vérifiez que vos informations d'identification de sécurité temporaires ne sont pas arrivées à expiration. Pour plus d'informations, consultez la section Demande d'informations d'identification de sécurité temporaires dans le guide de l'utilisateur IAM.

Résolution des problèmes de recherche dans Resource Explorer

Utilisez les informations fournies ici pour vous aider à diagnostiquer et à corriger les erreurs courantes qui peuvent survenir lorsque vous recherchez des ressources à l'aide de l'Explorateur de ressources.

Rubriques

Pourquoi certaines ressources ne figurent-elles pas dans les résultats de recherche de mon explorateur de ressources ?

La liste suivante indique les raisons pour lesquelles certaines ressources peuvent ne pas apparaître dans les résultats de recherche comme prévu :

L'indexation initiale n'est pas terminée

> Après avoir initialement activé l'Explorateur de ressources dans un Région AWS, l'indexation et la réplication vers l'index de l'agrégateur peuvent prendre jusqu'à 36 heures. Réessayez votre recherche ultérieurement.

La ressource est nouvelle

Quelques minutes peuvent être nécessaires pour qu'une nouvelle ressource soit découverte par Resource Explorer et ajoutée à l'index local. Réessayez dans quelques minutes.

Les informations relatives à une nouvelle ressource dans une région n'ont pas encore été propagées dans l'index agrégateur

Les détails d'une nouvelle ressource découverte dans une région peuvent prendre un certain temps pour être indexés dans sa propre région, puis répliqués dans l'index agrégateur du compte. La nouvelle ressource ne peut apparaître dans les résultats de recherche entre régions qu'une fois la réplication terminée. Réessayez votre recherche ultérieurement.

L'explorateur de ressources n'est pas activé dans la région où se trouve la ressource

Votre administrateur détermine dans quel Régions AWS environnement cet explorateur de ressources peut fonctionner. La page Paramètres indique les régions dans lesquelles l'explorateur de ressources est activé et contient un index. Si la région contenant votre ressource n'est pas activée, demandez à votre administrateur d'activer l'explorateur de ressources dans cette région.

La ressource existe dans une autre région et la région recherchée ne contient pas l'index agrégateur

Vous pouvez rechercher des ressources dans toutes les régions du compte uniquement en utilisant une vue de la région contenant l'index agrégateur. Les recherches effectuées dans une autre région renvoient uniquement les ressources de la région dans laquelle vous effectuez la recherche.

Les filtres de la vue excluent cette ressource

Chaque vue peut inclure des filtres dans la configuration qui limitent les résultats pouvant être inclus dans les résultats de recherche effectués avec cette vue. Assurez-vous que la ressource que vous recherchez correspond aux filtres de la vue que vous utilisez pour effectuer une recherche. Pour en savoir plus sur les filtres, consultezFiltres.

Le type de ressource n'est pas pris en charge par Resource Explorer

Certains types de ressources ne sont pas pris en charge par Resource Explorer. Pour de plus amples informations, veuillez consulter Types de ressources que vous pouvez rechercher avec Resource Explorer.

Les index ou les vues ne sont pas configurés dans la région de la console

Si les index ou les vues ne sont pas configurés dans les régions attendues par la console utilisant le widget, vous ne verrez pas les résultats escomptés. Pour de plus amples informations, veuillez consulter Activation de la recherche interrégionale en créant un index agrégateur.

Vos vues n'incluent pas les tags

Les balises sont requises par le widget Resource Explorer. Si vos vues n'incluent pas de balises, les ressources ne seront pas incluses dans vos résultats. Pour de plus amples informations, veuillez consulter L'ajout d'balises aux vues.

Votre recherche utilise la mauvaise syntaxe

La recherche dans l'explorateur de ressources est propre à ce service. Sans la syntaxe correcte, vous ne trouverez pas les ressources que vous attendez. Pour de plus amples informations, veuillez consulter Référence syntaxique des requêtes de recherche pour Resource Explorer.

Vous avez récemment tagué vos ressources

Une fois que vous avez marqué une ressource, un délai de 30 secondes s'écoule avant qu'elle n'apparaisse dans les résultats de recherche.

Le type de ressource ne prend pas en charge les filtres de balises

Si les filtres de balises ne sont pas pris en charge par le type de ressource, ils ne s'afficheront pas dans le widget Resource Explorer. Les types de ressources qui ne prennent pas en charge les filtres de balises sont les suivants :

- `cloudfront:cache-policy`
- `cloudfront:origin-access-identity`
- `cloudfront:function`
- `cloudfront:origin-request-policy`
- `cloudfront:realtime-log-config`
- `cloudfront:response-headers-policy`
- `cloudwatch:dashboard`
- `docdb:globalcluster`
- `elasticache:globalreplicationgroup`
- `iam:group`
- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `ssm:windowtarget`
- `ssm:windowtask`

- `rds:auto-backup`
- `rds:global-cluster`
- `s3:accesspoint`

Pourquoi mes ressources n'apparaissent-elles pas dans les résultats de recherche unifiés de la console ?

Les résultats de recherche unifiés sont disponibles dans la barre de recherche en haut de chaque AWS Management Console page. Toutefois, la recherche ne peut renvoyer des ressources correspondant à la requête dans les résultats de recherche qu'une fois les options de configuration suivantes terminées :

- Il doit y avoir un indice agrégateur dans l'une des régions du compte.
- Il doit y avoir une vue par défaut dans la région contenant l'index agrégateur.
- Tous les principaux (IAMrôles et utilisateurs) doivent être autorisés à effectuer des recherches à l'aide de cette vue par défaut.

Pourquoi la recherche unifiée dans la console et dans l'explorateur de ressources donne-t-elle parfois des résultats différents ?

Les résultats de recherche unifiés sont disponibles dans la barre de recherche en haut de chaque AWS Management Console page. Lorsque vous utilisez la recherche unifiée, le processus de recherche unifiée insère automatiquement un caractère générique (*) à la fin du premier terme saisi dans la chaîne de requête. Ce caractère générique n'est pas visible dans le champ de recherche unifié, mais il affecte les résultats.

> **Important**
>
> La recherche unifiée insère automatiquement un opérateur de caractère générique (*) à la fin du premier mot clé de la chaîne. Cela signifie que les résultats de recherche unifiés incluent des ressources correspondant à n'importe quelle chaîne commençant par le mot clé spécifié. La recherche effectuée par la zone de texte Requête sur la page de recherche de ressources de la console Resource Explorer n'ajoute pas automatiquement de caractère générique. Vous pouvez insérer un * manuellement après n'importe quel terme dans la chaîne de recherche.

De quelles autorisations ai-je besoin pour rechercher des ressources ?

Pour effectuer une recherche, vous devez être autorisé à effectuer les deux opérations suivantes sur une vue située dans la région dans laquelle vous appelez l'opération :

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

Cela peut être fait en ajoutant une déclaration similaire à l'exemple suivant à une politique attribuée à votre IAM directeur.

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

Vous pouvez remplacer le numéro de ressource Amazon (ARN) d'une vue spécifique par une vue ARN contenant un caractère générique (*) pour autoriser toutes les vues correspondantes.

Si vous ne spécifiez aucun affichage dans votre demande, Resource Explorer utilise automatiquement l'affichage par défaut pour la région dans laquelle vous avez fait la demande. Si vous n'êtes pas autorisé à utiliser l'affichage par défaut, contactez votre administrateur.

> **Note**
>
> Même si vous voyez une ressource dans les résultats d'une requête de recherche de l'explorateur de ressources, vous devez disposer d'autorisations sur la ressource elle-même pour pouvoir interagir avec cette ressource.

Quotas pour Resource Explorer

Vous avezCompte AWS des quotas par défaut pour chacun d'entre euxService AWS. Sauf indication contraire, les quotas sont spécifiques à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour afficher les quotas pourExplorateur de ressources AWS, ouvrez la boîte de dialogue Service Quotas. Dans le panneau de navigation, choisissez Services AWSet sélectionnez Resource Explorer.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

Les quotas suivants sont les valeurs par défaut de Resource Explorer.

Quotas de valeur maximaux	Valeur par défaut
Nombre de vues dans unRégion AWS	10

Limites de taux pour les opérations	Valeur par défaut
Nombre maximal d'opérations de recherche par seconde	5
Nombre maximal d'opérations non liées à la recherche par seconde	3
Nombre maximum d'opérations de recherche par mois dans la région agrégatrice	10 000
Nombre maximum d'opérations de recherche par mois dans les régions locales	500

Utilisation Explorateur de ressources AWS avec un AWS SDK

AWS des kits de développement logiciel (SDKs) sont disponibles pour de nombreux langages de programmation courants. Chacun SDK fournit des exemples de code et de la documentation qui permettent aux développeurs de créer plus facilement des applications dans leur langage préféré. API

SDKdocumentation	Exemples de code
AWS SDK pour C++	AWS SDK pour C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code
AWS SDK pour Kotlin	AWS SDK pour Kotlin exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code
Outils AWS pour PowerShell	Outils pour des exemples PowerShell de code
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Exemple de disponibilité

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

Historique du document pour le guide de l'utilisateur de Resource Explorer

Le tableau suivant décrit les versions de documentation pour Explorateur de ressources AWS. Pour recevoir des notifications concernant les mises à jour de cette documentation, vous pouvez vous abonner à un RSS flux.

Modification	Description	Date
Nouveau filtre de recherche ajouté	Resource Explorer a ajouté un nouveau filtre de requête de `tag:all` recherche, qui vous permet de rechercher des ressources associées à une ou plusieurs balises créées par l'utilisateur, même si le type de ressource n'est pas pris en charge dans Resource Explorer.	6 septembre 2024
Améliorations de l'organisation du	Titres de sujets mis à jour et contenu réorganisé pour améliorer la lisibilité et la découvrabilité.	29 août 2024
Avis de mise à niveau IAM des politiques vers IPv6	Les clients qui utilisent le double adressage avec des ASPEN politiques contenant des règles `aws:sourceIp` sont concernés par cette mise à niveau. Le double adressage signifie que le réseau prend en charge à la fois IPv4 etIPv6.	15 juillet 2024
Support interrompu pour trois types de ressources	Resource Explorer a cessé de prendre en charge les trois	9 juillet 2024

	types de ressources suivants : `ecs:tasks` `ssm:automation-execution` , `ssm:patchbaseline` .	
Ajout du support pour les nouveaux types de ressources	Resource Explorer a ajouté la prise en charge de 65 nouvelles ressources AWS Key Management Service, Services AWS notamment Amazon Route 53 et Amazon Fraud Detector.	20 février 2024
Mise à jour de la politique gérée	Resource Explorer a ajouté un support pour afficher des types de ressources supplémentaires. La politique `AWSResourceExplorerServiceRolePolicy` AWS gérée a été mise à jour pour autoriser l'explorateur de ressources à accéder à des types de ressources supplémentaires.	12 décembre 2023
Nouveau filtre de recherche ajouté	Resource Explorer prend désormais en charge la recherche de vos ressources par application.	16 novembre 2023
Ajout du support pour les nouveaux types de ressources	Resource Explorer a ajouté la prise en charge de 86 nouvelles ressources AWS CloudFormation, Services AWS notamment AWS Glue, et Amazon SageMaker.	15 novembre 2023

Resource Explorer prend en charge la recherche multi-comptes	Vous pouvez désormais utiliser l'Explorateur de ressources pour rechercher et découvrir des ressources Comptes AWS au sein de votre organisation ou de votre unité organisationnelle. Pour plus d'informations, consultez la section Activation de la recherche multi-comptes.	14 novembre 2023
Politiques gérées nouvelles et mises à jour	Resource Explorer a ajouté le support pour AWS Organizations. Les politiques AWS gérées ont été ajoutées et mises à jour pour accorder à Resource Explorer l'accès à votre organisation, à votre structure organisationnelle, à vos comptes et aux administrateurs délégués.	14 novembre 2023
Ajout du support pour les nouveaux types de ressources	Resource Explorer a ajouté le support pour AWS Organizations. Les politiques AWS gérées ont été mises à jour pour accorder à Resource Explorer l'accès à votre organisation, à votre structure organisationnelle, à vos comptes et aux administrateurs délégués.	14 novembre 2023

Ajout du support pour les nouveaux types de ressources	Resource Explorer prend désormais en charge 12 nouveaux types de ressource s provenant de services tels qu'Amazon Cognito et Amazon Elastic File System. AWS Elastic Beanstalk	18 octobre 2023
Ajout du support pour les nouveaux types de ressources	Resource Explorer a ajouté la prise en charge de 164 ressources. Les politiques AWS gérées qui accordent à Resource Explorer l'accès aux ressources d'index ont été mises à jour pour inclure ces nouveaux types de ressource s.	17 octobre 2023
L'explorateur de ressources est désormais disponible dans certaines régions optionnelles	Les clients BAH accèdent à Resource Explorer et CGK peuvent désormais s'y inscrire.	5 octobre 2023

Ajout du support pour les nouveaux types de ressources	Resource Explorer a ajouté la prise en charge des ressources suivantes Services AWS : AWS CodeBuild AWS CodePipeline, Amazon Cognito, Amazon Elastic Container Registry AWS Elastic Beanstalk, Amazon Elastic File System AWS IoT, et. AWS Step Functions Les politiques AWS gérées qui accordent à Resource Explorer l'accès aux ressources d'index ont été mises à jour pour inclure ces nouveaux types de ressources.	1er août 2023
Resource Explorer prend désormais en charge l'exportation des résultats de recherche vers CSV	Vous pouvez désormais exporter les résultats de votre recherche sur la page de recherche de ressources vers un fichier au CSV format - formaté.	4 avril 2023
Amazon Q Developer in chat applications À utiliser pour rechercher et découvrir vos AWS ressources	Vous pouvez désormais effectuer des recherches Amazon Q Developer in chat applications dans vos ressources à l'aide de questions en langage naturel. Pour plus d'informations, consultez la section Utilisation Amazon Q Developer in chat applications pour rechercher des ressources.	30 mars 2023

Ajout du support pour les nouveaux types de ressources	Resource Explorer a ajouté la prise en charge des ressources suivantes Services AWS : Amazon ElastiCache et Amazon Simple Queue Service (AmazonSQS). AWS Lambda Les politiques AWS gérées qui accordent à Resource Explorer l'accès aux ressources d'index ont été mises à jour pour inclure ces nouveaux types de ressources.	7 mars 2023
IAMmise à jour des meilleures pratiques	Guide mis à jour pour s'aligner sur les IAM meilleures pratiques. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité dans IAM.	6 décembre 2022
Nouvelles politiques AWS gérées	Resource Explorer ajoute AWSResourceExplorerFullAccess AWSResourceExplorerReadOnlyAccess et AWSResourceExplorerServiceRolePolicy gère des politiques.	7 novembre 2022
Première version	Publication initiale du guide de l'utilisateur de Resource Explorer	7 novembre 2022

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.