Guide de l'utilisateur

AWS Resource Groups

AWS Resource Groups: Guide de l’utilisateur

Table of Contents

Que sont les groupes de ressources ? ... 1
Les ressources et leurs types de groupes ... 1
Cas d'utilisation pour les groupes de ressources ... 3
AWS Resource Groups et autorisations ... 4
AWS Resource Groups ressources ... 4
Comment fonctionne le balisage ... 4
Premiers pas ... 5
Prérequis ... 6
Autorisation et contrôle d'accès aux Resource Groups ... 12
AWS des services qui fonctionnent avec AWS Resource Groups ... 13
Configurations de service ... 18
Accès ... 18
Syntaxe et structure ... 19
Types et paramètres de configuration ... 19
Création de groupes ... 36
Types de requêtes de groupes de ressources ... 36
Créez une requête basée sur des balises et créez un groupe ... 41
Création d'un groupe basé AWS CloudFormation sur une pile ... 43
Mise à jour de groupes ... 47
Mettre à jour les groupes de requêtes basés sur des balises ... 47
Mettre à jour un groupe AWS CloudFormation basé sur une pile ... 50
Surveillance des groupes de ressources pour détecter les modifications ... 54
Activation des événements du cycle de vie des groupes ... 56
Création d'une règle relative aux événements du cycle de vie des groupes ... 59
Création d'une règle pour capturer uniquement des types d'événements spécifiques du cycle de vie d'un groupe ... 61
Désactiver les événements du cycle de vie des groupes ... 62
Structure et syntaxe des événements ... 64
Structure du `detail` champ ... 65
Exemples de modèles d'événements personnalisés ... 73
Supprimer des groupes ... 77
Types de ressources pris en charge ... 78
Amazon API Gateway ... 80
Amazon API Gateway V2 ... 81

IAM Access Analyzer 81
AWS Amplify 81
AWS App Mesh 82
Amazon AppStream 82
AWS AppSync 83
Amazon Athena 83
AWS Backup 84
AWS Batch 84
AWS Billing Conductor 85
Amazon Braket 85
AWS Certificate Manager 86
AWS Certificate Manager Autorité de certification privée 86
AWS Cloud9 86
AWS CloudFormation 87
Amazon CloudFront 87
AWS Cloud Map 88
AWS CloudTrail 88
Amazon CloudWatch 89
Amazon CloudWatch Logs 89
Amazon CloudWatch Synthetics 90
AWS CodeArtifact 90
AWS CodeBuild 90
AWS CodeCommit 91
AWS CodeDeploy 91
CodeGuru Réviseur Amazon 92
Amazon CodeGuru Profiler 92
AWS CodePipeline 92
AWS CodeConnections 93
Amazon Cognito 93
Amazon Comprehend 94
AWS Config 94
Amazon Connect 95
Amazon Connect Wisdom 95
AWS Data Exchange 96
AWS Data Pipeline 96
AWS DataSync 96

AWS Database Migration Service 97
AWS Device Farm 97
Amazon DynamoDB 98
Amazon EMR 98
Conteneurs Amazon EMR 98
Amazon EMR sans serveur 99
Amazon ElastiCache 99
AWS Elastic Beanstalk 100
Amazon Elastic Compute Cloud (Amazon EC2) 100
Amazon Elastic Container Registry 105
Amazon Elastic Container Service 106
Amazon Elastic File System 106
Amazon Elastic Inference 107
Amazon Elastic Kubernetes Service (Amazon EKS) 107
Elastic Load Balancing 108
Amazon OpenSearch Service 108
CloudWatch Événements Amazon 109
EventBridge Schémas Amazon 109
Amazon FSx 110
Amazon Forecast 110
Amazon Fraud Detector 111
Amazon GameLift 112
AWS Global Accelerator 113
AWS Glue 113
AWS Glue DataBrew 114
AWS Ground Station 114
Amazon GuardDuty 115
Amazon Interactive Video Service 115
AWS Identity and Access Management 116
EC2 Image Builder 117
Amazon Inspector 117
AWS IoT 118
AWS IoT Analytics 119
AWS IoT Events 119
AWS IoT FleetWise 120
AWS IoT Greengrass 120

AWS IoT Greengrass Version 2 121
Console AWS IoT SiteWise 122
AWS IoT Wireless 122
AWS Key Management Service 123
Amazon Keyspaces (pour Apache Cassandra) 124
Amazon Kinesis 124
Service géré Amazon pour Apache Flink 124
Amazon Data Firehose 125
AWS Lambda 125
Amazon Lightsail 126
Amazon MQ 127
Amazon Macie 127
Amazon Managed Blockchain 128
Amazon Managed Streaming for Apache Kafka 128
AWS Elemental MediaConnect 128
AWS Elemental MediaPackage 129
AWS Network Manager 130
Amazon OpenSearch Service OpenSearch 130
AWS OpsWorks 131
AWS Organizations 131
Amazon Pinpoint 132
API de messages SMS et vocaux Amazon Pinpoint 132
Amazon Quantum Ledger Database (Amazon QLDB) 133
Amazon Redshift 133
Amazon Relational Database Service (Amazon RDS) 134
AWS Resource Access Manager 136
AWS Resource Groups 136
AWS Robomaker 136
Amazon Route 53 137
Amazon Route 53 Resolver 138
Amazon S3 Glacier 139
Amazon SageMaker 139
AWS Secrets Manager 141
AWS Service Catalog 141
AWS Service Catalog AppRegistry 142
Service Quotas 142

Amazon Simple Email Service ... 143
Amazon Simple Notification Service ... 143
Amazon Simple Queue Service ... 144
Amazon Simple Storage Service (Amazon S3) ... 144
AWS Step Functions ... 145
Storage Gateway ... 145
AWS Systems Manager ... 146
AWS Systems Manager pour SAP ... 146
Amazon Timestream ... 147
AWS Transfer Family ... 147
AWS WAF ... 148
Amazon WorkSpaces ... 148
AWS X-Ray ... 149
Types de ressources déconseillés ... 149
Création de groupes avec des AWS CloudFormation ressources ... 150
Resource Groups et AWS CloudFormation modèles ... 150
En savoir plus sur AWS CloudFormation ... 150
Sécurité ... 152
Protection des données ... 153
Chiffrement des données ... 154
Confidentialité du trafic inter-réseau ... 154
Gestion des identités et des accès ... 155
Public ciblé ... 155
Authentification par des identités ... 156
Gestion des accès à l'aide de politiques ... 159
Comment Resource Groups travaille avec IAM ... 162
Politiques gérées par AWS ... 167
Utilisation des rôles liés à un service ... 170
Exemples de politiques basées sur l'identité ... 173
Résolution des problèmes ... 178
Journalisation et surveillance ... 180
CloudTrail Intégration ... 180
Validation de conformité ... 183
Résilience ... 185
Sécurité de l'infrastructure ... 185
Bonnes pratiques de sécurité ... 186

Quotas de service 188
Historique de la documentation 189
Mises à jour antérieures 200
..... cci

Que sont les groupes de ressources ?

Vous pouvez utiliser des groupes de ressources pour organiser vos AWS ressources. AWS Resource Groups est le service qui vous permet de gérer et d'automatiser des tâches sur un grand nombre de ressources à la fois. Ce guide vous explique comment créer et gérer des groupes de ressources dans AWS Resource Groups. Les tâches que vous pouvez effectuer sur une ressource varient en fonction du AWS service que vous utilisez. Pour obtenir la liste des services pris en charge AWS Resource Groups et une brève description de ce que chaque service vous permet de faire avec un groupe de ressources, voirAWS des services qui fonctionnent avec AWS Resource Groups.

Vous pouvez accéder à Resource Groups via l'un des points d'entrée suivants.

- Dans AWS Management Consolela barre de navigation supérieure, sélectionnez Services. Ensuite, sous Management & Governance, choisissez Resource Groups & Tag Editor.

  Lien direct : AWS Resource Groups console
- En utilisant les Resource GroupsAPI, dans des AWS CLI commandes ou des langages AWS SDK de programmation. Consultez la AWS Resource Groups APIréférence pour plus d'informations.

Pour travailler avec des groupes de ressources à la AWS Management Console maison

1. Connectez-vous au AWS Management Console.
2. Dans la barre de navigation, choisissez Services.
3. Sous Management & Governance, sélectionnez Resource Groups & Tag Editor.
4. Dans le volet de navigation de gauche, choisissez Saved Resource Groups pour travailler avec un groupe existant ou Create a Group pour en créer un nouveau.

Les ressources et leurs types de groupes

Dans AWS, une ressource est une entité avec laquelle vous pouvez travailler. Les exemples incluent une EC2 instance Amazon, une AWS CloudFormation pile ou un compartiment Amazon S3. Si vous travaillez avec plusieurs ressources, il peut être utile de les gérer en groupe plutôt que de passer d'un AWS service à l'autre pour chaque tâche. Si vous gérez un grand nombre de ressources connexes, telles que EC2 des instances constituant une couche d'application, vous devrez probablement effectuer des actions groupées sur ces ressources en une seule fois. Les exemples d'actions en bloc incluent :

- L'application de mises à jour ou de correctifs de sécurité.
- La mise à niveau des applications
- L'ouverture ou la fermeture de ports au trafic réseau.
- La collecte de données de surveillance et de journaux spécifiques à partir de votre parc d'instances.

Un groupe de ressources est un ensemble de AWS ressources qui se trouvent toutes dans la même Région AWS entité et qui répondent aux critères spécifiés dans la requête du groupe. Dans Resource Groups, vous pouvez utiliser deux types de requêtes pour créer un groupe. Les deux types de requête incluent les ressources qui sont spécifiés dans le format `AWS::service::resource`.

- Basé sur des balises

  Un groupe de ressources basé sur des balises base son appartenance sur une requête qui spécifie une liste de types de ressources et de balises. Les balises sont des clés qui facilitent l'identification et le tri de vos ressources au sein de votre organisation. Le cas échéant, les balises incluent des valeurs pour les clés.

  > **Important**
  >
  > Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. Nous utilisons des tags pour vous fournir des services de facturation et d'administration. Les étiquettes ne sont pas destinées à être utilisées pour des données privées ou sensibles.

- AWS CloudFormation basé sur une pile

  Un groupe de ressources AWS CloudFormation basé sur une pile base son adhésion sur une requête qui indique une AWS CloudFormation pile dans votre compte dans la région actuelle. Vous pouvez éventuellement choisir les types de ressources dans la pile que vous souhaitez inclure dans le groupe. Vous ne pouvez baser votre requête que sur une seule AWS CloudFormation pile.

Groupes de ressources liés à un service

Certains Services AWS définissent des groupes de ressources que vous pouvez créer et gérer uniquement à l'aide de la console de ce service etAPIs. Vous êtes limité dans ce que vous pouvez faire avec ces groupes dans la console Resource Groups. Pour plus d'informations, consultez la

section Configurations de service pour les groupes de ressources dans le Guide de AWS Resource Groups API référence.

Les groupes de ressources peuvent être imbriqués ; un groupe de ressources peut contenir des groupes de ressources existantes dans la même région.

Cas d'utilisation pour les groupes de ressources

Par défaut, AWS Management Console il est organisé par AWS service. Mais avec Resource Groups, vous pouvez créer une console personnalisée qui organise et consolide les informations en fonction des critères spécifiés dans les balises ou des ressources d'une AWS CloudFormation pile. La liste suivante décrit certains des cas dans lesquels le regroupement des ressources facilite l'organisation de vos ressources.

- Une application avec différentes phases, par exemple, une phase de développement, une phase intermédiaire et une phase de production.
- Projets gérés par plusieurs services ou personnes.
- Ensemble de AWS ressources que vous utilisez ensemble pour un projet commun ou que vous souhaitez gérer ou surveiller en groupe.
- Un ensemble de ressources connexes aux applications s'exécutant sur une plateforme spécifique, comme Android ou iOS.

Par exemple, vous développez une application web et vous gérez des ensembles de ressources séparés pour vos étapes alpha, bêta et de mise en production. Chaque version fonctionne sur Amazon EC2 avec un volume de stockage Amazon Elastic Block Store. Vous utilisez Elastic Load Balancing pour gérer le trafic et Route 53 pour gérer votre domaine. Sans Resource Groups, il se peut que vous deviez accéder à plusieurs consoles uniquement pour vérifier l'état de vos services ou modifier les paramètres d'une version de votre application.

Avec Resource Groups, vous pouvez consulter et gérer vos ressources sur une seule page. Supposons, par exemple, que vous utilisiez l'outil pour créer un groupe de ressources pour chaque version (alpha, bêta et version) de votre application. Pour vérifier vos ressources pour la version alpha de votre application, ouvrez votre groupe de ressources. Les informations consolidées sont disponibles sur la page de votre groupe de ressources. Pour modifier une ressource spécifique, choisissez les liens de la ressource sur la page de votre groupe pour accéder rapidement à la console de service disposant des paramètres dont vous avez besoin.

AWS Resource Groups et autorisations

Les autorisations relatives à la fonctionnalité Resource Groups se situent au niveau du compte. Tant que IAM les principaux, tels que les rôles et les utilisateurs, qui partagent votre compte disposent des IAM autorisations appropriées, ils peuvent travailler avec les groupes de ressources que vous créez.

Les balises sont les propriétés d'une ressource. Elles sont donc partagées dans l'ensemble de votre compte. Les utilisateurs d'un service ou d'un groupe spécialisé peuvent se baser sur un vocabulaire (balises) commun au service ou au compte pour créer des groupes de ressources significatifs pour leurs rôles et responsabilités. Le fait de partager un pool de balises permet également aux utilisateurs qui partagent un groupe de ressources de ne plus avoir à se préoccuper du manque d'informations ou des conflits d'informations concernant les balises.

AWS Resource Groups ressources

Dans Resource Groups, la seule ressource disponible est un groupe. Les groupes sont associés à des noms de ressources Amazon (ARNs) uniques. Pour plus d'informations surARNs, consultez Amazon Resource Names (ARN) et les espaces de noms de AWS service dans le Référence générale d'Amazon Web Services.

Type de ressource	ARNFormater
Groupe de ressources	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`

Comment fonctionne le balisage

Les balises sont des paires clé/valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Pour la plupart des AWS ressources, vous avez la possibilité d'ajouter des balises lorsque vous créez la ressource, qu'il s'agisse d'une EC2 instance Amazon, d'un compartiment Amazon S3 ou d'une autre ressource. Cependant, vous pouvez également ajouter simultanément des balises à plusieurs ressources supportées à l'aide de Tag Editor. Vous créez une requête pour des ressources de différents types, puis ajoutez, supprimez ou remplacez des balises pour

les ressources de vos résultats de recherche. Les requêtes basées sur des balises attribuent un opérateur AND aux balises, afin que toutes les ressources correspondant aux types de ressources spécifiés et à toutes les balises spécifiées soient renvoyées par la requête.

> **Important**
>
> Ne stockez pas d'informations personnellement identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. Nous utilisons des tags pour vous fournir des services de facturation et d'administration. Les étiquettes ne sont pas destinées à être utilisées pour des données privées ou sensibles.

Pour plus d'informations sur le balisage, consultez le guide de l'utilisateur de l'éditeur de balises. Vous pouvez baliser les ressources prises en charge en utilisant Tag Editor ainsi que certaines ressources supplémentaires à l'aide d'une fonctionnalité de balisage dans la console de service dans laquelle vous créez et gérez la ressource.

Commencer avec AWS Resource Groups

Dans AWS, une ressource est une entité avec laquelle vous pouvez travailler. Les exemples incluent une EC2 instance Amazon, un compartiment Amazon S3 ou une zone hébergée Amazon Route 53. Si vous travaillez avec plusieurs ressources, il peut être utile de les gérer en groupe plutôt que de passer d'un AWS service à l'autre pour chaque tâche.

Cette section vous montre comment démarrer AWS Resource Groups. Tout d'abord, organisez les AWS ressources en les balisant dans l'éditeur de balises. Créez ensuite des requêtes dans Resource Groups qui incluent les types de ressources que vous souhaitez inclure dans un groupe et les balises que vous avez appliquées aux ressources.

Après avoir créé des groupes de ressources dans Resource Groups, utilisez AWS Systems Manager des outils tels que Automation pour simplifier les tâches de gestion de vos groupes de ressources.

Pour plus d'informations sur la prise en main des AWS Systems Manager fonctionnalités et des outils, consultez le guide de AWS Systems Manager l'utilisateur.

Rubriques

- Conditions préalables pour travailler avec AWS Resource Groups
- En savoir plus sur AWS Resource Groups l'autorisation et le contrôle d'accès

Conditions préalables pour travailler avec AWS Resource Groups

Avant de commencer à travailler avec des groupes de ressources, assurez-vous d'avoir un AWS compte avec les ressources existantes et les droits appropriés pour étiqueter les ressources et créer des groupes.

Rubriques

- Inscrivez-vous pour AWS
- Créer des ressources
- Configuration d'autorisations

Inscrivez-vous pour AWS

Si vous n'avez pas de 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, une Utilisateur racine d'un compte AWSest créé. L'utilisateur root a accès à tous Services AWS et les ressources du 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.

Créer des ressources

Vous pouvez créer un groupe de ressources vide, mais vous ne pourrez effectuer aucune tâche sur les membres du groupe de ressources tant qu'il n'y aura pas de ressources dans le groupe. Pour plus d'informations sur les types de ressources pris en charge, consultez Types de ressources que vous pouvez utiliser avec AWS Resource Groups l'éditeur de balises.

Configuration d'autorisations

Pour exploiter pleinement les groupes de ressources et Tag Editor, vous pouvez avoir besoin d'autorisations supplémentaires pour baliser les ressources ou pour consulter les valeurs et les clés de balise d'une ressource. Ces autorisations de lancement sont réparties en plusieurs catégories :

- Les autorisations pour les services individuels, afin de pouvoir baliser des ressources à partir de ces services et les inclure dans des groupes de ressources.
- Autorisations requises pour utiliser la console Tag Editor
- Autorisations requises pour utiliser le AWS Resource Groups console etAPI.

Si vous êtes administrateur, vous pouvez accorder des autorisations à vos utilisateurs en créant des politiques via le AWS Identity and Access Management (IAM) service. Vous devez d'abord créer vos principes, tels que les IAM rôles ou les utilisateurs, ou associer des identités externes à votre AWS environnement utilisant un service tel que AWS IAM Identity Center. Vous appliquez ensuite des politiques avec les autorisations dont vos utilisateurs ont besoin. Pour plus d'informations sur la création et IAM l'attachement de politiques, consultez la section Utilisation des politiques.

Autorisations pour des services individuels

> **Important**
>
> Cette section décrit les autorisations requises si vous souhaitez étiqueter des ressources provenant d'autres consoles de service et APIs ajouter ces ressources à des groupes de ressources.

Comme décrit dans Les ressources et leurs types de groupes, chaque groupe de ressources représente un ensemble de ressources de types spécifiés qui partagent une ou plusieurs valeurs ou clés de balise. Pour ajouter des balises à une ressource, vous devez disposer des autorisations nécessaires pour le service auquel appartient la ressource. Par exemple, pour étiqueter des EC2 instances Amazon, vous devez être autorisé à effectuer les actions de balisage dans le cadre de ces servicesAPI, telles que celles répertoriées dans le guide de l'EC2utilisateur Amazon.

Pour utiliser pleinement la fonction Groupes de ressources, vous avez besoin d'autres autorisations qui vous permettent d'accéder à la console d'un service, où vous pourrez interagir avec les ressources. Pour des exemples de telles politiques pour AmazonEC2, consultez la section Exemples de politiques pour travailler dans la EC2 console Amazon dans le guide de EC2 l'utilisateur Amazon.

Autorisations requises pour Resource Groups et Tag Editor

Pour utiliser Resource Groups et Tag Editor, les autorisations suivantes doivent être ajoutées à la déclaration de politique d'un utilisateur dansIAM. Vous pouvez ajouter soit AWS-politiques gérées qui sont maintenues et conservées up-to-date par AWS, ou vous pouvez créer et gérer votre propre politique personnalisée.

Utilisation AWS politiques gérées pour les autorisations Resource Groups et Tag Editor

AWS Resource Groups et Tag Editor prennent en charge les éléments suivants AWS des politiques gérées que vous pouvez utiliser pour fournir un ensemble prédéfini d'autorisations à vos utilisateurs. Vous pouvez associer ces politiques gérées à n'importe quel utilisateur, rôle ou groupe comme vous le feriez pour toute autre politique que vous créez.

ResourceGroupsandTagEditorReadOnlyAccess

Cette politique accorde au IAM rôle ou à l'utilisateur attaché l'autorisation d'appeler les opérations en lecture seule pour Resource Groups et Tag Editor. Pour lire les balises d'une ressource, vous devez également disposer d'autorisations pour cette ressource par le biais d'une politique distincte (voir la note importante suivante).

ResourceGroupsandTagEditorFullAccess

Cette politique accorde au IAM rôle ou à l'utilisateur attaché l'autorisation d'appeler n'importe quelle opération Resource Groups et les opérations de lecture et d'écriture de balises dans Tag Editor. Pour lire ou écrire les balises d'une ressource, vous devez également disposer d'autorisations pour cette ressource par le biais d'une politique distincte (voir la note importante suivante).

> **Important**
>
> Les deux politiques précédentes accordent l'autorisation d'appeler les opérations Resource Groups et Tag Editor et d'utiliser ces consoles. Pour les opérations Resource Groups, ces politiques sont suffisantes et accordent toutes les autorisations nécessaires pour utiliser n'importe quelle ressource dans la console Resource Groups.
> Toutefois, pour les opérations de balisage et la console Tag Editor, les autorisations sont plus détaillées. Vous devez disposer des autorisations non seulement pour invoquer l'opération, mais également des autorisations appropriées pour la ressource spécifique dont vous essayez d'accéder aux balises. Pour accorder cet accès aux balises, vous devez également joindre l'une des politiques suivantes :

- Le AWS-managed policy ReadOnlyAccessaccorde des autorisations aux opérations en lecture seule pour les ressources de chaque service. AWS tient automatiquement cette politique à jour avec les nouvelles AWS services dès qu'ils sont disponibles.
- De nombreux services fournissent un service en lecture seule spécifique au service AWS- des politiques gérées que vous pouvez utiliser pour limiter l'accès aux seules ressources fournies par ce service. Par exemple, Amazon EC2 fournit Amazon EC2ReadOnlyAccess.
- Vous pouvez créer votre propre politique qui n'accorde l'accès qu'à des opérations de lecture seule très spécifiques pour les quelques services et ressources auxquels vous souhaitez que vos utilisateurs accèdent. Cette politique utilise soit une stratégie de « liste d'autorisation », soit une stratégie de liste de refus.

  Une stratégie de liste d'autorisation tire parti du fait que l'accès est refusé par défaut tant que vous ne l'autorisez pas explicitement dans une politique. Vous pouvez donc utiliser une politique comme dans l'exemple suivant :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

  Vous pouvez également utiliser une stratégie de « liste de refus » qui autorise l'accès à toutes les ressources, à l'exception de celles que vous bloquez explicitement.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
```

```
}
```

Ajouter manuellement les autorisations Resource Groups et Tag Editor

- `resource-groups:*`(Cette autorisation autorise toutes les actions Resource Groups. Si vous souhaitez plutôt restreindre les actions accessibles à un utilisateur, vous pouvez remplacer l'astérisque par une action Resource Groups spécifique (ou par une liste d'actions séparées par des virgules).
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

> **Note**
>
> L'`resource-groups:SearchResources`autorisation permet à Tag Editor de répertorier les ressources lorsque vous filtrez votre recherche à l'aide de clés ou de valeurs de balise. L'`resource-explorer:ListResources`autorisation permet à l'éditeur de balises de répertorier les ressources lorsque vous recherchez des ressources sans définir de balises de recherche.

Pour utiliser Resource Groups et Tag Editor dans la console, vous devez également être autorisé à exécuter l'`resource-groups:ListGroupResources`action. Cette autorisation est nécessaire pour répertorier les types de ressources disponibles dans la région actuelle. L'utilisation de conditions de politique avec n'`resource-groups:ListGroupResources`est actuellement pas prise en charge.

Octroi d'autorisations d'utilisation AWS Resource Groups et éditeur de balises

Pour ajouter une politique d'utilisation AWS Resource Groups et Tag Editor pour un utilisateur, procédez comme suit.

1. Ouvrez la IAMconsole.
2. Dans le panneau de navigation, choisissez utilisateurs.
3. Trouvez l'utilisateur à qui vous souhaitez octroyer AWS Resource Groups et autorisations de l'éditeur de balises. Choisissez le nom d'utilisateur pour ouvrir la page des propriétés de l'utilisateur.
4. Choisissez Ajouter des autorisations.
5. Choisissez Attach existing policies directly (Attacher directement les politiques existantes).
6. Choisissez Create Policy (Créer une politique).
7. JSONDans l'onglet, collez la déclaration de politique suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Cet exemple de déclaration de politique accorde des autorisations uniquement pour AWS Resource Groups et actions de l'éditeur de balises. Il ne permet pas l'accès à AWS Systems Manager tâches dans le AWS Resource Groups console. Par exemple, cette politique ne vous autorise pas à utiliser les commandes d'automatisation de Systems Manager. Pour exécuter des tâches de Systems Manager sur des groupes de ressources, vous devez disposer des autorisations Systems Manager associées

à votre politique (par exemple`ssm:*`). Pour plus d'informations sur l'octroi de l'accès à Systems Manager, voir Configuration de l'accès à Systems Manager dans le AWS Systems Manager Guide de l'utilisateur.

8. Choisissez Review policy (Examiner une politique).
9. Donnez à la nouvelle stratégie un nom et une description (par exemple, `AWSResourceGroupsQueryAPIAccess`).
10. Choisissez Create Policy (Créer une politique).
11. Maintenant que la politique est enregistréeIAM, vous pouvez l'associer à d'autres utilisateurs. Pour plus d'informations sur la façon d'ajouter une politique à un utilisateur, voir Ajouter des autorisations en attachant des politiques directement à l'utilisateur dans le Guide de IAM l'utilisateur.

En savoir plus sur AWS Resource Groups l'autorisation et le contrôle d'accès

Resource Groups prend en charge les solutions suivantes.

- Stratégies basées sur une action. Par exemple, vous pouvez créer une politique qui autorise les utilisateurs à effectuer des ListGroupsopérations, mais pas d'autres.
- Autorisations au niveau des ressources. Resource Groups prend en charge l'utilisation ARNspour spécifier des ressources individuelles dans la politique.
- Autorisation basée sur des tags. Resource Groups prend en charge l'utilisation de balises de ressources dans le cadre d'une politique. Par exemple, vous pouvez créer une politique qui permet aux utilisateurs de Resource Groups d'accéder pleinement à un groupe que vous avez balisé.
- Informations d'identification temporaires. Les utilisateurs peuvent assumer un rôle dans le cadre d'une politique autorisant les AWS Resource Groups opérations.

Resource Groups ne prend pas en charge les politiques basées sur les ressources.

Pour plus d'informations sur la manière dont Resource Groups et Tag Editor s'intègrent à AWS Identity and Access Management (IAM), consultez les rubriques suivantes du guide de AWS Identity and Access Management l'utilisateur.

- AWS des services qui fonctionnent avec IAM

- Actions, ressources et clés de condition pour AWS Resource Groups
- Contrôle de l'accès à l'aide de politiques

AWS des services qui fonctionnent avec AWS Resource Groups

Vous pouvez utiliser les AWS services suivants avec AWS Resource Groups.

AWS service	Utilisation avec Resource Groups
AWS CloudFormation— Créez des groupes de ressources à AWS CloudFormation l'aide d'un modèle de pile.	Fournir et organiser AWS les ressources en même temps. Organisez les ressources par balises. Organisez les ressources provenant d'une autre pile. Collectez des informations sur vos AWS ressources dans des groupes de ressources à l'aide d'Amazon CloudWatch ou prenez des mesures opérationnelles à l'aide de AWS Systems Manager. Pour plus d'informations, consultez la référence ResourceGroups aux types de ressources dans le Guide de AWS CloudFormation l'utilisateur.
CloudTrail— Capturez toutes les actions des groupes de ressources à l'aide de AWS CloudTrail.	Capturez des informations sur les actions effectuées sur vos groupes de ressources, notamment des informations telles que l'auteur de l'action (principal IAM, tel qu'un rôle, un utilisateur ou un Service AWS), le moment où l'action a été effectuée, le lieu où l'action s'est produite (l'adresse IP source), etc. Ces enregistrements peuvent ensuite être utilisés à des fins d'analyse ou pour déclencher des actions de suivi. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

AWS service	Utilisation avec Resource Groups
Amazon CloudWatch — Activez la surveillance en temps réel de vos AWS ressources et des applications que vous utilisez AWS.	Concentrez votre affichage pour afficher les métriques et les alarmes provenant d'un seul groupe de ressources. Pour plus d'informations, consultez la section Concentrez-vous sur les métriques et les alarmes dans un groupe de ressources dans le guide de CloudWatch l'utilisateur Amazon.
Amazon CloudWatch Application Insights : détectez les problèmes courants liés à vos applications .NET et SQL Server.	Surveillez les ressources de vos applicati ons .NET et SQL Server qui appartiennent à un groupe de ressources. Pour plus d'informations, consultez la section Composants d'application pris en charge dans le guide de CloudWatch l'utilisateur Amazon.
Groupes de tables Amazon DynamoDB : organisez vos tables DynamoDB en groupes logiques afin de gérer plus facilement vos ressources.	Créez, modifiez et supprimez des groupes de tables DynamoDB à partir du menu Action DynamoDB. Pour plus d'informations, consultez le guide du développeur Amazon DynamoDB.
Hôtes dédiés Amazon EC2 : utilisez vos licences logicielles existantes par socket, par cœur ou par machine virtuelle, notamment Windows Server, Microsoft SQL Server, SUSE et Linux Enterprise Server.	Lancez des instances Amazon EC2 dans des groupes de ressources hôtes pour optimiser votre utilisation des hôtes dédiés. Pour plus d'informations, consultez la section Travailler avec des hôtes dédiés dans le guide de l'utilisateur Amazon EC2.

AWS service	Utilisation avec Resource Groups
Réservations de capacité Amazon EC2 : réservez de la capacité pour vos instances Amazon EC2 à utiliser lorsque vous en avez besoin. Vous pouvez spécifier des attributs pour la réservation de capacité afin qu'elle ne fonctionne qu'avec les instances Amazon EC2 lancées avec des attributs correspondants.	Lancez vos instances Amazon EC2 dans des groupes de ressources contenant une ou plusieurs réservations de capacité. Si le groupe ne dispose pas d'une réservation de capacité avec les attributs correspondants et la capacité disponible pour une instance demandée, celle-ci s'exécute en tant qu'instance à la demande. Si vous ajoutez ultérieurement une réservati on de capacité correspondante au groupe cible, l'instance est automatiquement mise en correspondance avec la capacité réservée et déplacée vers celle-ci. Pour plus d'informations, consultez la section Travailler avec des groupes de réservation de capacité dans le guide de l'utilisateur Amazon EC2.
AWS License Manager— Simplifiez le processus de transfert des licences des fournisseurs de logiciels vers le cloud.	Configurez un groupe de ressources d'hôtes pour permettre à License Manager de gérer vos hôtes dédiés. Pour plus d'informations, consultez Host Resource Groups in License Manager dans le Guide de l'utilisateur du License Manager.
AWS Resilience Hub — Préparez et protégez vos applications contre les perturbations.	Découvrez vos applications définies à l'aide de Resource Groups. Pour plus d'informations, consultez Mesurer et améliorer la résilience de vos applications avec AWS Resilience Hub dans le blog d'AWS actualités.

AWS service	Utilisation avec Resource Groups
AWS Resource Access Manager— Partagez AWS des ressources spécifiques que vous possédez avec d'autres comptes.	Partagez des groupes de ressources hôtes à l'aide de AWS RAM. Pour plus d'informations, consultez la section Ressources partageables dans le Guide de l'AWS RAM utilisateur.
AWS Service Catalog AppRegistry— Définissez et gérez vos applications et leurs métadonnées.	Lorsque vous créez une application dans AppRegistry, ce service crée automatiquement un groupe de ressources pour cette application. Le groupe de ressources de l'application est un ensemble de toutes les ressources de votre application. Le service crée également un groupe de ressources AWS CloudFormation basé sur une pile pour chaque pile associée à l'application. Pour plus d'informations, consultez la section Utilisation AppRegistry dans le guide de AWS Service Catalog l'administrateur.

AWS service	Utilisation avec Resource Groups
AWS Systems Manager— Améliorez la visibilité et le contrôle de vos AWS ressources.	Collectez des informations opérationnelles et effectuez des actions groupées sur vos applications en fonction de groupes de ressources. Dans la AWS Systems Manager console, la page Applications personnalisées d'Application Manager importe et affiche automatiquement les données d'opérati ons pour les applications basées sur des groupes de ressources. Vous pouvez utiliser les informations contenues dans le gestionna ire d'applications pour vous aider à détermine r quelles ressources d'une application sont conformes et fonctionnent correctement et quelles ressources nécessitent une action. Pour plus d'informations, consultez la section Utilisation des applications dans le Gestionna ire d'applications dans le Guide de AWS Systems Manager l'utilisateur.
Analyseur d'accès réseau Amazon VPC — Identifiez les accès réseau indésirables à vos ressources sur. AWS	Vous pouvez spécifier les sources et les destinations correspondant à vos besoins d'accès au réseau en utilisant AWS Resource Groups. Cela vous permet de gérer l'accès au réseau dans l'ensemble de votre AWS environnement, indépendamment de la façon dont vous configurez votre réseau. Pour plus d'informations, consultez Use Resource Groups with Network Access Scopes dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Configurations de service pour les groupes de ressources

Les groupes de ressources vous permettent de gérer les collections de vos AWS ressources en tant qu'unité. Certains AWS services prennent en charge cela en effectuant les opérations demandées sur tous les membres du groupe. Ces services peuvent stocker les paramètres à appliquer aux membres du groupe sous forme de configuration sous la forme d'une structure de JSONdonnées attachée au groupe.

Cette rubrique décrit les paramètres de configuration disponibles pour les AWS services pris en charge.

Rubriques

- Comment accéder à la configuration de service attachée à un groupe de ressources
- JSONsyntaxe d'une configuration de service
- Types et paramètres de configuration pris en charge

Comment accéder à la configuration de service attachée à un groupe de ressources

Les services qui prennent en charge les groupes liés à des services définissent généralement la configuration pour vous lorsque vous utilisez les outils fournis par ce service, tels que la console de gestion de ce service ou ses opérations AWS CLI . AWS SDK Certains services gèrent entièrement leurs groupes liés aux services et vous ne pouvez pas les modifier, sauf dans les limites autorisées par la console ou par les commandes fournies par le service propriétaire AWS . Toutefois, dans certains cas, vous pouvez interagir avec la configuration du service en utilisant les API opérations suivantes dans le AWS SDKs ou leurs AWS CLI équivalents :

- Vous pouvez associer votre propre configuration à un groupe lorsque vous créez le groupe à l'aide de l'CreateGroupopération.
- Vous pouvez modifier la configuration actuelle attachée à un groupe à l'aide de cette PutGroupConfigurationopération.
- Vous pouvez consulter la configuration actuelle d'un groupe de ressources en appelant l'GetGroupConfigurationopération.

JSONsyntaxe d'une configuration de service

Un groupe de ressources peut contenir une configuration qui définit les paramètres spécifiques au service qui s'appliquent aux ressources membres de ce groupe.

Une configuration est exprimée sous forme d'JSONobjet. Au niveau le plus élevé, une configuration est un ensemble d'éléments de configuration de groupe. Chaque élément de configuration de groupe contient deux éléments : un `Type` pour la configuration et un ensemble `Parameters` défini par ce type. Chaque paramètre contient un `Name` et un tableau d'un ou plusieurs paramètres`Values`. L'exemple suivant avec *`placeholders`* montre la syntaxe de base d'une configuration pour un seul type de ressource d'échantillon. Cet exemple montre un type avec deux paramètres, et chaque paramètre avec deux valeurs. Les types, paramètres et valeurs valides réels sont décrits dans la section suivante.

```
[
    {
        "Type": "configuration-type",
        "Parameters": [
            {
                "Name": "parameter1-name",
                "Values": [
                    "value1",
                    "value2"
                ]
            },
            {
                "Name": "parameter2-name",
                "Values": [
                    "value3",
                    "value4"
                ]
            }
        ]
    }
]
```

Types et paramètres de configuration pris en charge

Resource Groups prend en charge l'utilisation des types de configuration suivants. Chaque type de configuration possède un ensemble de paramètres valides pour ce type.

Rubriques

- AWS::ResourceGroups::Generic
- AWS::AppRegistry::Application
- AWS::CloudFormation::Stack
- AWS::EC2::CapacityReservationPool
- AWS::EC2::HostManagement
- AWS::NetworkFirewall::RuleGroup

`AWS::ResourceGroups::Generic`

Ce type de configuration spécifie les paramètres qui appliquent les exigences d'adhésion au groupe de ressources, plutôt que de configurer le comportement d'un type de ressource spécifique pour un AWS service. Ce type de configuration est automatiquement ajouté par les groupes liés aux services qui en ont besoin, tels que les types `AWS::EC2::CapacityReservationPool` et`AWS::EC2::HostManagment`.

Les éléments suivants `Parameters` sont valides pour le groupe `AWS::ResourceGroups::Generic` lié à un service. `Type`

- **`allowed-resource-types`**

  Ce paramètre indique que le groupe de ressources ne peut être composé que de ressources du ou des types spécifiés.

  Type de données des valeurs : Chaîne

  Valeurs autorisées :

  - `AWS::EC2::Host`— Un A `Configuration` avec ce paramètre et cette valeur est requis lorsque la configuration du service contient également un type `Configuration` of`AWS::EC2::HostManagement`. Cela garantit que le `HostManagement` groupe ne peut contenir que des hôtes EC2 dédiés Amazon.
  - `AWS::EC2::CapacityReservation`— Un A `Configuration` avec ce paramètre et cette valeur est requis lorsque la configuration du service contient également un `Configuration` élément de type`AWS::EC2::CapacityReservationPool`. Cela garantit qu'un `CapacityReservation` groupe ne peut contenir que des EC2 capacités de réservation d'Amazon.

Obligatoire : conditionnel, basé sur d'autres `Configuration` éléments attachés au groupe de ressources. Consultez l'entrée précédente pour les valeurs autorisées.

L'exemple suivant limite les membres du groupe aux seules instances EC2 hôtes Amazon.

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            }
        ]
    }
]
```

- **`deletion-protection`**

  Ce paramètre indique que le groupe de ressources ne peut être supprimé que s'il ne contient aucun membre. Pour plus d'informations, voir Supprimer un groupe de ressources hôtes dans le Guide de l'utilisateur de License Manager

  Type de données de valeurs : Tableau de chaînes

  Valeurs autorisées : La seule valeur autorisée est `[ "UNLESS_EMPTY" ]` (la valeur doit être en majuscules).

  Obligatoire : conditionnel, basé sur d'autres `Configuration` éléments attachés au groupe de ressources. Ce paramètre n'est obligatoire que lorsque le groupe de ressources possède également un autre `Configuration` élément portant le nom `Type` de`AWS::EC2::HostManagement`.

  L'exemple suivant active la protection contre la suppression pour le groupe, sauf si le groupe ne compte aucun membre.

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
```

```
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

AWS::AppRegistry::Application

Ce `Configuration` type indique que le groupe de ressources représente une application créée par AWS Service Catalog AppRegistry.

Les groupes de ressources de ce type sont entièrement gérés par le AppRegistry service et ne peuvent être créés, mis à jour ou supprimés par les utilisateurs qu'à l'aide des outils fournis par AppRegistry.

> **Note**
>
> Étant donné que les groupes de ressources de ce type sont automatiquement créés et gérés par l'utilisateur AWS et ne sont pas gérés par celui-ci, ils ne sont pas pris en compte dans votre limite de quota pour le nombre maximum de groupes de ressources que vous pouvez créer dans votre Compte AWS.

Pour plus d'informations, consultez la section Utilisation AppRegistry dans le Guide de l'utilisateur du Service Catalog.

Lors de la AppRegistry création d'un groupe de ressources lié à un service de ce type, il crée également automatiquement un groupe AWS CloudFormation lié à un service distinct et supplémentaire pour chaque AWS CloudFormation pile associée à l'application.

AppRegistry nomme automatiquement les groupes liés à un service de ce type qu'il crée avec le préfixe `AWS_AppRegistry_Application-` suivi du nom de l'application : `AWS_AppRegistry_Application-`*`MyAppName`*

Les paramètres suivants sont pris en charge pour le type de groupe `AWS::AppRegistry::Application` lié à un service.

- **`Name`**

Ce paramètre spécifie le nom convivial de l'application qui a été attribué par l'utilisateur lors de sa création dans AppRegistry.

Type de données des valeurs : Chaîne

Valeurs autorisées : toute chaîne de texte autorisée par le AppRegistry service pour le nom d'une application.

Obligatoire : oui

- **`Arn`**

  Ce paramètre spécifie le chemin Amazon Resource Name (ARN) de l'application attribué par AppRegistry.

  Type de données des valeurs : Chaîne

  Valeurs autorisées : validesARN.

  Obligatoire : oui

> **Note**
>
> Pour modifier l'un de ces éléments, vous devez modifier l'application à l'aide de la AppRegistry console ou des AWS CLI opérations AWS SDK de ce service.

Ce groupe de ressources d'applications inclut automatiquement en tant que membres du groupe les groupes de ressources créés pour les AWS CloudFormation piles associées à l' AppRegistry application. Vous pouvez utiliser cette ListGroupResourcesopération pour voir ces groupes d'enfants.

L'exemple suivant montre à quoi ressemble la section de configuration d'un groupe `AWS::AppRegistry::Application` lié à un service.

```
[
    {
        "Type": "AWS::AppRegistry::Application",
        "Parameters":[
            {
```

```
                "Name": "Name",
                "Values": [
                    "MyApplication"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
                ]
            }
        ]
    }
]
```

AWS::CloudFormation::Stack

Ce `Configuration` type indique que le groupe représente une AWS CloudFormation pile et que ses membres sont les AWS ressources créées par cette pile.

Les groupes de ressources de ce type sont automatiquement créés pour vous lorsque vous AWS CloudFormation associez une pile au AppRegistry service. Vous ne pouvez pas créer, mettre à jour ou supprimer ces groupes si ce n'est en utilisant les outils fournis par AppRegistry.

AppRegistry nomme automatiquement les groupes liés à un service de ce type qu'il crée avec le préfixe `AWS_CloudFormation_Stack-` suivi du nom de la pile : `AWS_CloudFormation_Stack-`*`MyStackName`*

> **Note**
>
> Étant donné que les groupes de ressources de ce type sont automatiquement créés et gérés par l'utilisateur AWS et ne sont pas gérés par celui-ci, ils ne sont pas pris en compte dans votre limite de quota pour le nombre maximum de groupes de ressources que vous pouvez créer dans votre Compte AWS.

Pour plus d'informations, consultez la section Utilisation AppRegistry dans le Guide de l'utilisateur du Service Catalog.

AppRegistry crée automatiquement un groupe de ressources lié à un service de ce type pour chaque AWS CloudFormation pile que vous associez à l' AppRegistry application. Ces groupes de ressources deviennent des membres enfants du groupe de ressources parent de l' AppRegistryapplication.

Les membres de ce groupe de AWS CloudFormation ressources sont les AWS ressources créées dans le cadre de la pile.

Les paramètres suivants sont pris en charge pour le type de groupe `AWS::CloudFormation::Stack` lié à un service.

- **`Name`**

  Ce paramètre indique le nom convivial de la AWS CloudFormation pile attribué par l'utilisateur lors de sa création.

  Type de données des valeurs : Chaîne

  Valeurs autorisées : toute chaîne de texte autorisée par le AWS CloudFormation service pour un nom de pile.

  Obligatoire : oui

- **`Arn`**

  Ce paramètre spécifie le chemin Amazon Resource Name (ARN) de la AWS CloudFormation pile attachée à l'application dans AppRegistry.

  Type de données des valeurs : Chaîne

  Valeurs autorisées : validesARN.

  Obligatoire : oui

> **Note**
>
> Pour modifier l'un de ces éléments, vous devez modifier l'application à l'aide de la AppRegistry console ou d'un équivalent AWS SDK et AWS CLI des opérations.

L'exemple suivant montre à quoi ressemble la section de configuration d'un groupe `AWS::CloudFormation::Stack` lié à un service.

```
[
    {
        "Type": "AWS::CloudFormation::Stack",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyStack"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
                ]
            }
        ]
    }
]
```

`AWS::EC2::CapacityReservationPool`

Ce `Configuration` type indique que le groupe de ressources représente un pool commun de capacités fourni par les membres du groupe. Les membres de ce groupe de ressources doivent obligatoirement effectuer des réservations de EC2 capacité auprès d'Amazon. Un groupe de ressources peut inclure à la fois des réservations de capacité que vous possédez sur votre compte et des réservations de capacité partagées avec vous à partir d'autres comptes en utilisant AWS Resource Access Manager. Cela vous permet de lancer une EC2 instance Amazon en utilisant ce groupe de ressources comme valeur pour le paramètre de réservation de capacité. Dans ce cas, l'instance utilise la capacité réservée disponible dans le groupe. Si le groupe de ressources n'a aucune capacité disponible, l'instance est lancée en tant qu'instance autonome à la demande en dehors du pool. Pour plus d'informations, consultez la section Travailler avec des groupes de réservation de capacité dans le guide de EC2 l'utilisateur Amazon.

Si vous configurez un groupe de ressources lié à un service avec un `Configuration` élément de ce type, vous devez également spécifier des `Configuration` éléments distincts avec les valeurs suivantes :

- Un `AWS::ResourceGroups::Generic` type avec un seul paramètre :
  - Le paramètre `allowed-resource-types` et une valeur unique de`AWS::EC2::CapacityReservation`. Cela garantit que seules les réservations EC2 de capacité Amazon peuvent être membres du groupe de ressources.

L'`AWS::EC2::CapacityReservationPool`élément d'une configuration de groupe ne prend en charge aucun paramètre.

L'exemple suivant montre à quoi ressemble la `Configuration` section d'un tel groupe.

```
[
    {
        "Type": "AWS::EC2::CapacityReservationPool"
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::CapacityReservation" ]
            }
        ]
    }
]
```

`AWS::EC2::HostManagement`

Cet identifiant spécifie les paramètres de gestion des EC2 hôtes Amazon et AWS License Manager qui sont appliqués aux membres du groupe. Pour plus d'informations, consultez la section Groupes de ressources hôtes dans AWS License Manager.

Si vous configurez un groupe de ressources lié à un service avec un `Configuration` élément de ce type, vous devez également spécifier des `Configuration` éléments distincts avec les valeurs suivantes :

- Un `AWS::ResourceGroups::Generic` type, avec un paramètre `allowed-resource-types` et une valeur unique de`AWS::EC2::Host`. Cela garantit que seuls les hôtes EC2 dédiés Amazon peuvent être membres du groupe.

- Un `AWS::ResourceGroups::Generic` type, avec un paramètre `deletion-protection` et une valeur unique de`UNLESS_EMPTY`. Cela garantit que le groupe ne peut être supprimé que s'il est vide.

Les paramètres suivants sont pris en charge pour le type de groupe `AWS::EC2::HostManagement` lié à un service.

- **`auto-allocate-host`**

  Ce paramètre indique si les instances sont lancées sur un hôte dédié spécifique ou sur un hôte disponible doté d'une configuration correspondante. Pour plus d'informations, consultez la section Comprendre le placement automatique et l'affinité dans le guide de EC2 l'utilisateur Amazon.

  Type de données des valeurs : booléen

  Valeurs autorisées : « vrai » ou « faux » (doit être en minuscules).

  Obligatoire : non

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": [ "true" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
```

```
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **`auto-release-host`**

  Ce paramètre indique si un hôte dédié du groupe est automatiquement libéré après l'arrêt de sa dernière instance en cours d'exécution. Pour plus d'informations, consultez la section Releasing Dedicated Hosts dans le guide de EC2 l'utilisateur Amazon.

  Type de données des valeurs : booléen

  Valeurs autorisées : « vrai » ou « faux » (doit être en minuscules).

  Obligatoire : non

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-release-host",
                "Values": [ "false" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
```

```
        ]
    }
]
```

- **`allowed-host-families`**

  Ce paramètre indique quelles familles de types d'instances peuvent être utilisées par les instances membres de ce groupe.

  Type de données de valeurs : un tableau de chaînes.

  Valeurs autorisées : chacune doit être un identifiant de famille de type d'EC2instance Amazon valide`C4`, tel que`M5`,`P3dn`, ou`R5d`.

  Obligatoire : non

  L'exemple d'élément de configuration suivant indique que les instances lancées ne peuvent être membres que des familles de types d'instances C5 ou M5.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
```

```
            }
        ]
    }
]
```

- **`allowed-host-based-license-configurations`**

  Ce paramètre spécifie les chemins Amazon Resource Name (ARN) d'une ou de plusieurs configurations de licence basées sur le noyau/le socket que vous souhaitez appliquer aux membres du groupe.

  Type de données de valeurs : un tableau deARNs.

  Valeurs autorisées : chacune doit être une configuration de License Manager valideARN.

  Obligatoire : selon les conditions. Vous devez spécifier soit ce paramètre`any-host-based-license-configuration`, soit les deux. Ils s'excluent mutuellement.

  L'exemple d'élément de configuration suivant indique que les membres du groupe peuvent utiliser les deux configurations de License Manager spécifiées.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
```

```
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **`any-host-based-license-configuration`**

  Ce paramètre indique que vous ne souhaitez pas associer une configuration de licence spécifique à votre groupe. Dans ce cas, toutes les configurations de licence basées sur le noyau/le socket sont disponibles pour les membres de votre groupe de ressources hôte. Utilisez ce paramètre si vous disposez d'un nombre illimité de licences et que vous souhaitez optimiser l'utilisation de l'hôte.

  Type de données des valeurs : booléen

  Valeurs autorisées : « vrai » ou « faux » (doit être en minuscules).

  Obligatoire : selon les conditions. Vous devez spécifier soit ce paramètre`allowed-host-based-license-configurations`, soit les deux. Ils s'excluent mutuellement.

  L'exemple d'élément de configuration suivant indique que les membres du groupe peuvent utiliser n'importe quelle configuration de licence basée sur le noyau/le socket.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
```

```
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

L'exemple suivant montre comment inclure tous les paramètres de gestion de l'hôte dans une configuration unique.

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": ["true"]
            },
            {
                "Name": "auto-release-host",
                "Values": ["false"]
            },
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
```

```
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

AWS::NetworkFirewall::RuleGroup

Cet identifiant spécifie les paramètres des groupes de AWS Network Firewall règles qui sont appliqués aux membres du groupe. Les administrateurs de pare-feu peuvent spécifier le nom ARN d'un groupe de ressources de ce type afin de résoudre automatiquement les adresses IP des membres du groupe pour une règle de pare-feu au lieu d'avoir à répertorier chaque adresse manuellement. Pour plus d'informations, consultez la section Utilisation de groupes de ressources basés sur des balises dans AWS Network Firewall.

Vous pouvez créer des groupes de ressources de ce type de configuration à l'aide de la console Network Firewall ou en exécutant une AWS CLI commande ou une AWS SDK opération.

Les groupes de ressources de ce type de configuration sont soumis aux restrictions suivantes :

- Les membres du groupe se composent uniquement de ressources dont les types sont pris en charge par Network Firewall.
- Le groupe doit contenir une requête basée sur des balises pour gérer les membres du groupe ; toutes les ressources des types pris en charge dont les balises correspondent à la requête sont automatiquement membres du groupe.
- Ce type de configuration n'est pas `Parameters` pris en charge.
- Pour supprimer un groupe de ressources de ce type de configuration, aucun groupe de règles Network Firewall ne peut le référencer.

L'exemple suivant illustre les `ResourceQuery` sections `Configuration` et pour un groupe de ce type.

```
{
    "Configuration": [
        {
```

```
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

L'exemple de AWS CLI commande suivant crée un groupe de ressources avec la configuration et la requête précédentes.

```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
        "OwnerId":"123456789012"
    },
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

Création de groupes basés sur des requêtes dans AWS Resource Groups

Types de requêtes de groupes de ressources

Dans AWS Resource Groups, une requête est le fondement d'un groupe basé sur des requêtes. Vous pouvez baser un groupe de ressources sur l'un des deux types de requêtes.

Basé sur des balises

Les requêtes basées sur des balises incluent des listes de types de ressources spécifiés dans le format suivant`AWS::service::resource`, ainsi que des balises. Les balises sont des clés qui facilitent l'identification et le tri de vos ressources au sein de votre organisation. Le cas échéant, les balises incluent des valeurs pour les clés.

Pour une requête basée sur une balise, vous pouvez également spécifier les balises qui sont partagés par les ressources dont vous souhaitez qu'elles soient membres du groupe. Par exemple, si vous souhaitez créer un groupe de ressources contenant toutes les EC2 instances Amazon et les compartiments Amazon S3 que vous utilisez pour exécuter la phase de test d'une application, et que vous avez des instances et des compartiments balisés de cette façon, choisissez les types de `AWS::S3::Bucket` ressources `AWS::EC2::Instance` et dans la liste déroulante, puis spécifiez la clé de balise**`Stage`**, avec une valeur de balise de. **`Test`**

La syntaxe du `ResourceQuery` paramètre d'un groupe de ressources basé sur des balises contient les éléments suivants :

- `Type`

  Cet élément indique le type de requête qui définit ce groupe de ressources. Pour créer un groupe de ressources basé sur des balises, spécifiez la valeur `TAG_FILTERS_1_0` comme suit :

  ```
  "Type": "TAG_FILTERS_1_0"
  ```

- `Query`

Cet élément définit la requête réelle utilisée pour établir une correspondance avec les ressources. Il contient une représentation sous forme de chaîne d'une JSON structure avec les éléments suivants :

- `ResourceTypeFilters`

  Cet élément limite les résultats aux seuls types de ressources qui correspondent au filtre. Vous pouvez spécifier les valeurs suivantes :

  - `"AWS::AllSupported"`— pour spécifier que les résultats peuvent inclure des ressources de tout type correspondant à la requête et actuellement prises en charge par le service Resource Groups.
  - `"AWS::`*`service-id`*`::`*`resource-type`*— une liste séparée par des virgules de chaînes de spécification de type ressource au format suivant :, par exemple. `"AWS::EC2::Instance"`

- `TagFilters`

  Cet élément spécifie les paires de chaînes clé/valeur qui sont comparées aux balises associées à vos ressources. Les personnes dont la clé de balise et la valeur correspondent au filtre sont incluses dans le groupe. Chaque filtre est composé des éléments suivants :

  - `"Key"`— une chaîne avec un nom de clé. Seules les ressources dotées de balises avec un nom de clé correspondant correspondent au filtre et sont membres du groupe.
  - `"Values"`— une chaîne avec une liste de valeurs séparées par des virgules pour la clé spécifiée. Seules les ressources dont la clé de balise correspond et dont la valeur correspond à l'une des ressources de cette liste sont membres du groupe.

Tous ces JSON éléments doivent être combinés dans une représentation sous forme de chaîne sur une seule ligne de la JSON structure. Par exemple, considérez a `Query` avec l'exemple de JSON structure suivant. Cette requête est destinée à faire correspondre uniquement les EC2 instances Amazon dont le tag « Stage » est associé à la valeur « Test ».

```
{
    "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
    "TagFilters": [
        {
            "Key": "Stage",
            "Values": [ "Test" ]
        }
    ]
```

```
}
```

Cela JSON peut être représenté sous la forme de la chaîne d'une seule ligne suivante et utilisé comme valeur de l'`Query`élément. Comme la valeur d'une JSON structure doit être une chaîne entre guillemets doubles, vous devez éviter les guillemets ou les barres obliques intégrés en les faisant précéder d'une barre oblique inverse, comme indiqué ici :

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":
\"Stage\",\"Values\":[\"Test\"]}]}"
```

La `ResourceQuery` chaîne complète est ensuite représentée comme indiqué ici, en tant que paramètre de CLI commande :

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters\":
[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

AWS CloudFormation basé sur une pile

Dans une requête AWS CloudFormation basée sur une pile, vous choisissez une AWS CloudFormation pile dans votre compte dans la région actuelle, puis vous choisissez les types de ressources dans la pile que vous souhaitez inclure dans le groupe. Vous ne pouvez baser votre requête que sur une seule AWS CloudFormation pile.

> **Note**
>
> Une AWS CloudFormation pile peut contenir d'autres piles AWS CloudFormation « enfants ». Cependant, un groupe de ressources basé sur une pile « parent » n'obtient pas toutes les ressources des piles enfants en tant que membres du groupe. Les groupes de ressources ajoutent les piles enfants au groupe de ressources de la pile parent en tant que membres individuels du groupe et ne les développent pas.

Resource Groups prend en charge les requêtes basées sur des AWS CloudFormation piles présentant l'un des statuts suivants.

- `CREATE_COMPLETE`
- `CREATE_IN_PROGRESS`
- `DELETE_FAILED`

- `DELETE_IN_PROGRESS`
- `REVIEW_IN_PROGRESS`

> **Important**
>
> Seules les ressources directement créées dans le cadre de la pile de la requête sont incluses dans le groupe de ressources. Les ressources créées ultérieurement par les membres de la AWS CloudFormation pile ne deviennent pas membres du groupe. Par exemple, si un groupe d'auto-scaling est créé par dans le AWS CloudFormation cadre de la pile, ce groupe d'auto-scaling en est membre. Toutefois, une EC2 instance Amazon créée par ce groupe d'auto-scaling dans le cadre de son fonctionnement n'est pas membre du groupe de ressources basé sur une AWS CloudFormation pile.

Si vous créez un groupe basé sur une AWS CloudFormation pile et que le statut de la pile change pour devenir un groupe qui n'est plus pris en charge comme base pour une requête de groupe, par exemple`DELETE_COMPLETE`, le groupe de ressources existe toujours, mais il ne possède aucune ressource membre.

Après avoir créé un groupe de ressources, vous pouvez effectuer des tâches sur les ressources du groupe.

La syntaxe du `ResourceQuery` paramètre d'un groupe de ressources CloudFormation basé sur une pile contient les éléments suivants :

- `Type`

  Cet élément indique le type de requête qui définit ce groupe de ressources.

  Pour créer un groupe de ressources AWS CloudFormation basé sur une pile, spécifiez la valeur comme `CLOUDFORMATION_STACK_1_0` suit :

  ```
  "Type": "CLOUDFORMATION_STACK_1_0"
  ```

- `Query`

  Cet élément définit la requête réelle utilisée pour établir une correspondance avec les ressources. Il contient une représentation sous forme de chaîne d'une JSON structure avec les éléments suivants :

- `ResourceTypeFilters`

  Cet élément limite les résultats aux seuls types de ressources qui correspondent au filtre. Vous pouvez spécifier les valeurs suivantes :

  - `"AWS::AllSupported"`— pour spécifier que les résultats peuvent inclure des ressources de tout type correspondant à la requête.
  - `"AWS::`*`service-id`*`::`*`resource-type`*— une liste séparée par des virgules de chaînes de spécification de type ressource au format suivant :, par exemple. `"AWS::EC2::Instance"`

- `StackIdentifier`

  Cet élément indique le nom de ressource Amazon (ARN) de la AWS CloudFormation pile dont vous souhaitez inclure les ressources dans le groupe.

Tous ces JSON éléments doivent être combinés dans une représentation sous forme de chaîne sur une seule ligne de la JSON structure. Par exemple, considérez a `Query` avec l'exemple de JSON structure suivant. Cette requête est destinée à correspondre uniquement aux compartiments Amazon S3 qui font partie de la AWS CloudFormation pile spécifiée.

```
{
    "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
    "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

Cela JSON peut être représenté sous la forme de la chaîne d'une seule ligne suivante et utilisé comme valeur de l'`Query`élément. Comme la valeur d'une JSON structure doit être une chaîne entre guillemets doubles, vous devez éviter les guillemets ou les barres obliques intégrés en les faisant précéder d'une barre oblique inverse, comme indiqué ici :

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/MyCloudFormationStackName\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\"
```

La `ResourceQuery` chaîne complète est ensuite représentée comme indiqué ici, en tant que paramètre de CLI commande :

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":\"arn:aws:cloudformation:us-
west-2:123456789012:stack\/MyCloudFormationStackName\/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\"}'
```

Créez une requête basée sur des balises et créez un groupe

Les procédures suivantes vous montrent comment créer une requête basée sur des balises et l'utiliser pour créer un groupe de ressources.

Console

1. Connectez-vous à la console AWS Resource Groups.
2. Dans le volet de navigation, choisissez Create Resource Group.
3. Sur la page Créer un groupe basé sur des requêtes, sous Type de groupe, choisissez le type de groupe basé sur des balises.
4. Sous Critères de regroupement, choisissez les types de ressources que vous souhaitez inclure dans votre groupe de ressources. Vous pouvez avoir un maximum de 20 types de ressources dans une requête. Pour cette procédure pas à pas, choisissez AWS: : EC2 : :Instance et ::S3 AWS : :Bucket.
5. Toujours sous Critères de regroupement, pour les balises, spécifiez une clé de balise, ou une paire clé-valeur de balise, afin de limiter les ressources correspondantes afin d'inclure uniquement celles qui sont étiquetées avec les valeurs que vous avez spécifiées. Choisissez Add (Ajouter) ou appuyez sur Enter (Entrée) lorsque vous avez terminé votre balise. Dans cet exemple, filtrez les ressources disposant d'une clé de balise Stage (Étape). La valeur de balise est facultative, mais affine les résultats de la requête. Vous pouvez ajouter plusieurs valeurs pour une clé de balise en ajoutant un `OR` opérateur entre les valeurs de balise. Choisissez Add (Ajouter) pour ajouter plus de balises. Les requêtes attribuent un opérateur `AND` aux balises, afin que toutes les ressources correspondant aux types de ressources spécifiés et à toutes les balises spécifiées soient renvoyées par la requête.
6. Toujours sous Critères de regroupement, choisissez Prévisualiser les ressources du groupe pour renvoyer la liste des EC2 instances et des compartiments S3 de votre compte qui correspondent à la ou aux clés de balise spécifiées.
7. Une fois que vous avez obtenu les résultats souhaités, créez un groupe basé sur cette requête.

a. Sous Détails du groupe, dans Nom du groupe, tapez le nom de votre groupe de ressources.

   Un nom de groupe de ressources peut avoir un maximum de 128 caractères, y compris des lettres, des chiffres, des tirets, des points et des traits de soulignement. Le nom ne peut pas commencer par `AWS` ou `aws`. Ils sont réservés. Le nom d'un groupe de ressources doit être unique dans la région actuelle de votre compte.

b. (Facultatif) Dans Group description (Description du groupe), saisissez une description de votre groupe.

c. (Facultatif) Dans Group tags (Balises du groupe), ajoutez des paires de clés et de valeurs de balise qui s'appliquent uniquement au groupe de ressources, et non aux ressources membres du groupe.

   Les balises de groupe sont utiles si vous envisagez de faire de ce groupe un membre d'un groupe plus important. Veillez à ajouter au moins une clé de balise dans Group tags (Balises de groupe) aux groupes que vous envisagez d'imbriquer dans des groupes plus importants, car vous devez spécifier au moins une clé de balise pour créer un groupe.

8. Lorsque vous avez terminé, choisissez Créer un groupe.

AWS CLI & AWS SDKs

Un groupe basé sur des balises est basé sur une requête de type `TAG_FILTERS_1_0`.

1. Dans une AWS CLI session, tapez ce qui suit, puis appuyez sur Entrée pour remplacer les valeurs du nom du groupe, de la description, des types de ressources, des clés de balise et des valeurs de balise par les vôtres. Les descriptions peuvent avoir un maximum de 512 caractères, y compris des lettres, des chiffres, des tirets, des traits de soulignement, des signes de ponctuation et des espaces. Vous pouvez avoir un maximum de 20 types de ressources dans une requête. Un nom de groupe de ressources peut avoir un maximum de 128 caractères, y compris des lettres, des chiffres, des tirets, des points et des traits de soulignement. Le nom ne peut pas commencer par `AWS` ou `aws`. Ils sont réservés. Un nom de groupe de ressources doit être unique dans votre compte.

   Au moins une valeur pour `ResourceTypeFilters` est obligatoire. Pour spécifier tous les types de ressources, utilisez `AWS::AllSupported` en tant que valeur `ResourceTypeFilters`.

```
$ aws resource-groups create-group \
    --name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

Voici un exemple de commande.

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":
[\"Test\"]}]}"}'
```

La commande suivante est un exemple qui inclut tous les types de ressources pris en charge.

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

2. Les éléments suivants sont renvoyés dans la réponse à la commande.
   - Une description complète du groupe que vous avez créé.
   - La requête de ressources que vous avez utilisée pour créer le groupe.
   - Les balises associées au groupe.

Création d'un groupe basé AWS CloudFormation sur une pile

Les procédures suivantes vous montrent comment créer une requête basée sur une pile et comment l'utiliser pour créer un groupe de ressources.

Console

1. Connectez-vous à la console AWS Resource Groups.
2. Dans le volet de navigation, choisissez Create Resource Group.

3. Dans Créer un groupe basé sur une requête, sous Type de groupe, choisissez le type de groupe basé sur une CloudFormation pile.
4. Choisissez la pile dont vous souhaitez faire la base de votre groupe. Un groupe de ressources peut être basé sur une seule pile. Pour filtrer la liste des piles, commencez par taper le nom de la pile. Seuls les piles avec des états pris en charge apparaissent dans la liste.
5. Choisissez des types de ressource dans la pile que vous souhaitez inclure dans le groupe. Pour cette procédure pas à pas, conservez la valeur par défaut, tous les types de ressources pris en charge. Pour plus d'informations sur les types de ressources qui sont pris en charge et peuvent faire partie du groupe, consultez Types de ressources que vous pouvez utiliser avec AWS Resource Groups l'éditeur de balises.
6. Choisissez Afficher les ressources du groupe pour renvoyer la liste des ressources de la AWS CloudFormation pile correspondant aux types de ressources que vous avez sélectionnés.
7. Une fois que vous avez obtenu les résultats souhaités, créez un groupe basé sur cette requête.

   a. Sous Détails du groupe, dans Nom du groupe, tapez le nom de votre groupe de ressources.

      Un nom de groupe de ressources peut avoir un maximum de 128 caractères, y compris des lettres, des chiffres, des tirets, des points et des traits de soulignement. Le nom ne peut pas commencer par `AWS` ou `aws`. Ils sont réservés. Le nom d'un groupe de ressources doit être unique dans la région actuelle de votre compte.

   b. (Facultatif) Dans Group description (Description du groupe), saisissez une description de votre groupe.

   c. (Facultatif) Dans Group tags (Balises du groupe), ajoutez des paires de clés et de valeurs de balise qui s'appliquent uniquement au groupe de ressources, et non aux ressources membres du groupe.

      Les balises de groupe sont utiles si vous envisagez de faire de ce groupe un membre d'un groupe plus important. Veillez à ajouter au moins une clé de balise dans Group tags (Balises de groupe) aux groupes que vous envisagez d'imbriquer dans des groupes plus importants, car vous devez spécifier au moins une clé de balise pour créer un groupe.

8. Lorsque vous avez terminé, choisissez Créer un groupe.

AWS CLI & AWS SDKs

Un groupe AWS CloudFormation basé sur une pile est basé sur une requête de type. `CLOUDFORMATION_STACK_1_0`

1. Exécutez la commande suivante en remplaçant les valeurs du nom du groupe, de la description, de l'identifiant de pile et des types de ressources par les vôtres. Les descriptions peuvent avoir un maximum de 512 caractères, y compris des lettres, des chiffres, des tirets, des traits de soulignement, des signes de ponctuation et des espaces.

   Si vous ne spécifiez aucun type de ressource, Resource Groups inclut tous les types de ressources pris en charge dans la pile. Vous pouvez avoir un maximum de 20 types de ressources dans une requête. Un nom de groupe de ressources peut avoir un maximum de 128 caractères, y compris des lettres, des chiffres, des tirets, des points et des traits de soulignement. Le nom ne peut pas commencer par `AWS` ou `aws`. Ils sont réservés. Un nom de groupe de ressources doit être unique dans votre compte.

   Le *`stack_identifier`* est la pileARN, comme indiqué dans l'exemple de commande.

```
$ aws resource-groups create-group \
    --name group_name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

   Voici un exemple de commande.

```
$ aws resource-groups create-group \
    --name My-CFN-stack-group \
    --description "My first CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

2. Les éléments suivants sont renvoyés dans la réponse à la commande.

   - Une description complète du groupe que vous avez créé.

- La requête de ressources que vous avez utilisée pour créer le groupe.

Mettre à jour des groupes dans AWS Resource Groups

Pour mettre à jour un groupe de ressources basé sur des balises dans Resource Groups, vous pouvez modifier la requête et les balises qui constituent la base de votre groupe. Vous pouvez ajouter et supprimer des ressources de votre groupe uniquement en modifiant la requête ou les balises. Vous ne pouvez pas sélectionner des ressources spécifiques à ajouter ou à supprimer de votre groupe. La meilleure façon d'ajouter ou de supprimer une ressource spécifique dans un groupe est de modifier les balises de la ressource. Vérifiez ensuite que votre requête de balise de groupe de ressources inclut ou omet la balise, selon que vous souhaitez que la ressource soit incluse dans votre groupe.

Pour mettre à jour un groupe de ressources AWS CloudFormation basé sur une pile, vous pouvez choisir une autre pile. Vous pouvez également ajouter ou supprimer des types de ressources de la pile dont vous souhaitez faire partie du groupe. Pour modifier les ressources disponibles dans la pile, mettez à jour le AWS CloudFormation modèle utilisé pour créer la pile, puis mettez à jour la pile AWS CloudFormation. Pour plus d'informations sur la mise à jour d'une AWS CloudFormation pile, consultez la section Mises à jour AWS CloudFormation des piles dans le Guide de AWS CloudFormation l'utilisateur.

Dans le AWS CLI, vous mettez à jour les groupes à l'aide de deux commandes.

- `update-group`, que vous exécutez pour mettre à jour la description d'un groupe.
- `update-group-query`, que vous exécutez pour mettre à jour la requête d'une ressource et les balises qui déterminent les ressources membres du groupe.

Dans la console, vous ne pouvez pas transformer un groupe AWS CloudFormation basé sur une pile en un groupe de requêtes basé sur des balises, ou vice versa. Toutefois, vous pouvez le faire en utilisant les Resource GroupsAPI, notamment dans le AWS CLI.

Mettre à jour les groupes de requêtes basés sur des balises

Les procédures suivantes indiquent comment mettre à jour un groupe de requêtes basé sur des balises.

Console

Mettre à jour un groupe basé sur des balises en modifiant les types de ressources ou des balises dans la requête sur laquelle le groupe est basé. Vous pouvez également ajouter ou modifier la description du groupe.

1. Connectez-vous à la console AWS Resource Groups.
2. Dans le volet de navigation, sous Saved Resource Groups, choisissez le nom du groupe, puis choisissez Edit.

> **Note**
>
> Vous ne pouvez mettre à jour que les groupes de ressources dont vous êtes le propriétaire. La colonne Propriétaire indique la propriété du compte pour chaque groupe de ressources. Tous les groupes dont le propriétaire du compte est autre que celui auquel vous êtes connecté ont été créés AWS License Manager. Pour plus d'informations, consultez la section Groupes de ressources Host AWS License Manager dans le Guide de l'utilisateur du License Manager.

3. Sur la page Modifier le groupe, sous Critères de regroupement, ajoutez ou supprimez des types de ressources. Vous pouvez avoir un maximum de 20 types de ressources dans une requête. Pour supprimer un type de ressources, choisissez X sur l'étiquette du type de ressources. Choisissez View group resources (Afficher les ressources du groupe) pour voir en quoi les modifications affectent les ressources membres du groupe. Dans cette procédure pas à pas, nous ajoutons le type de ressource AWS: : RDS : : DBInstance à la requête.
4. Toujours sous Critères de regroupement, modifiez les balises selon vos besoins. Dans cet exemple, nous filtrons les ressources disposant d'une clé de balise Stage (Étape) et ajoutons une valeur de balise Test. La valeur de balise est facultative, mais affine les résultats de la requête. Pour supprimer une balise, choisissez X sur la balise de l'étiquette.
5. Dans Additional information (Informations supplémentaires), vous pouvez modifier la description du groupe. Vous ne pouvez pas modifier un nom du groupe une fois que le groupe a été créé.
6. (Facultatif) Dans Grouper les balises, vous pouvez ajouter ou supprimer des balises. Les balises de groupe sont des métadonnées sur votre groupe de ressources. Elles n'affectent pas les ressources membres. Pour modifier les ressources renvoyées par la requête du groupe de ressources, modifiez les balises situées sous Critères de regroupement.

   Les balises de groupe sont utiles si vous envisagez de faire de ce groupe un membre d'un groupe plus important. La spécification d'au moins une clé de balise est requise pour créer un groupe. Par conséquent, veillez à ajouter au moins une clé de balise dans les balises de groupe aux groupes que vous prévoyez d'imbriquer dans des groupes plus importants.

7. Choisissez Preview group resources pour récupérer la liste mise à jour des EC2 instances, des compartiments S3 et des instances de RDS base de données Amazon de votre compte qui correspondent aux clés de balise spécifiées. Si vous ne voyez pas les ressources que vous attendez dans la liste, veillez à ce qu'elles soient balisées avec des balises que vous avez spécifiées dans la zone Grouping criteria (Critères de regroupement).
8. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

AWS CLI & AWS SDKs

Dans le AWS CLI, vous mettez à jour la requête d'un groupe et la description d'un groupe de ressources à l'aide de deux commandes différentes. Vous ne pouvez pas modifier un nom de groupe existant. Dans le AWS CLI, vous pouvez transformer un groupe basé sur des balises en un groupe basé CloudFormation sur une pile, ou vice versa.

1. Si vous ne souhaitez pas modifier la description de votre groupe, ignorez cette étape et passez à la suivante. Dans une AWS CLI session, tapez ce qui suit, puis appuyez sur Entrée pour remplacer les valeurs du nom et de la description du groupe par les vôtres.

```
$ aws resource-groups update-group \
    --group-name resource-group-name \
    --description "description_text"
```

   Voici un exemple de commande.

```
$ aws resource-groups update-group \
    --group-name my-resource-group \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

   La commande renvoie une description mise à jour complète du groupe.

2. Pour mettre à jour la requête et les balises d'un groupe, tapez la commande suivante. Remplacez les valeurs du nom du groupe, des types de ressources, des clés de balise et des valeurs de balise par les vôtres. Appuyez ensuite sur Entrée. Vous pouvez avoir un maximum de 20 types de ressources dans une requête.

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
```

```
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

Voici un exemple de commande.

```
$ aws resource-groups update-group-query \
    --group-name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test\"]}]}"}'
```

La commande renvoie la requête mise à jour comme résultat.

Mettre à jour un groupe AWS CloudFormation basé sur une pile

Les procédures suivantes indiquent comment mettre à jour un groupe CloudFormation basé sur une pile.

Console

Vous ne pouvez pas remplacer un groupe AWS CloudFormation basé sur une pile par un groupe basé sur des balises dans le. AWS Management Console Toutefois, vous pouvez modifier la pile sur laquelle le groupe est basé ou modifier les types de ressources de pile que vous souhaitez inclure dans le groupe. Vous pouvez également ajouter ou modifier la description du groupe.

1. Connectez-vous à la console AWS Resource Groups.
2. Dans le volet de navigation, sous Groupes de ressources enregistrés, choisissez le nom du groupe, puis sélectionnez Modifier.
3.

> **Note**
>
> Vous ne pouvez mettre à jour que les groupes de ressources dont vous êtes le propriétaire. La colonne Propriétaire indique la propriété du compte pour chaque groupe de ressources. Tous les groupes dont le propriétaire du compte est autre que celui auquel vous êtes connecté ont été créés AWS License Manager. Pour

plus d'informations, consultez la section Groupes de ressources Host AWS License Manager dans le Guide de l'utilisateur du License Manager.

4. Sur la page Modifier le groupe, sous Critères de regroupement, pour modifier la pile sur laquelle est basé votre groupe, choisissez la pile dans la liste déroulante. Un groupe de ressources peut être basé sur une seule pile. Pour filtrer la liste des piles, commencez par taper le nom de la pile. Seuls les piles avec des états pris en charge apparaissent dans la liste. Pour obtenir une liste des statuts pris en charge, consultez la section Création de groupes basés sur des requêtes dans AWS Resource Groups de ce guide.
5. Ajouter ou supprimer des types de ressources. Seuls les types de ressource qui sont disponibles dans la pile sont affichés dans la liste déroulante. La valeur par défaut est All supported resource types (Tous les types de ressources pris en charge). Vous pouvez avoir un maximum de 20 types de ressources dans une requête. Pour supprimer un type de ressources, choisissez X sur l'étiquette du type de ressources. Pour plus d'informations sur les types de ressources qui sont pris en charge et peuvent faire partie du groupe, consultez Types de ressources que vous pouvez utiliser avec AWS Resource Groups l'éditeur de balises.
6. Choisissez Prévisualiser les ressources du groupe pour récupérer la liste des ressources de la AWS CloudFormation pile correspondant aux types de ressources que vous avez sélectionnés.
7. Dans Additional information (Informations supplémentaires), vous pouvez modifier la description du groupe. Vous ne pouvez pas modifier un nom du groupe une fois que le groupe a été créé.
8. Dans Group tags (Balises de groupe), ajouter ou supprimer des balises. Les balises de groupe sont des métadonnées sur votre groupe de ressources. Elles n'affectent pas les ressources membres. Pour modifier les ressources renvoyées par la requête du groupe de ressources, modifiez les balises dans la zone Grouping criteria (Critères de regroupement).

   Les balises de groupe sont utiles si vous envisagez de faire de ce groupe un membre d'un groupe plus important. La spécification d'au moins une clé de balise est requise pour créer un groupe. Par conséquent, veillez à ajouter au moins une clé de balise dans les balises de groupe aux groupes que vous prévoyez d'imbriquer dans des groupes plus importants.
9. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

AWS CLI & AWS SDKs

Dans le AWS CLI, vous mettez à jour la requête d'un groupe et la description d'un groupe de ressources à l'aide de deux commandes différentes. Vous ne pouvez pas modifier un nom de groupe existant. Dans le AWS CLI, vous pouvez transformer un groupe basé sur des balises en un groupe basé CloudFormation sur une pile, ou vice versa.

1. Si vous ne souhaitez pas modifier la description de votre groupe, ignorez cette étape et passez à la suivante. Exécutez la commande suivante en remplaçant les valeurs du nom et de la description du groupe par les vôtres.

   ```
   $ aws resource-groups update-group \
       --group-name "resource-group-name" \
       --description "description_text"
   ```

   Voici un exemple de commande.

   ```
   $ aws resource-groups update-group \
       --group-name "My-CFN-stack-group" \
       --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
    the test stage."
   ```

   La commande renvoie une description mise à jour complète du groupe.

2. Pour mettre à jour la requête et les balises d'un groupe, exécutez la commande suivante. Remplacez les valeurs du nom du groupe, de l'identifiant de pile et des types de ressources par les vôtres. Pour ajouter des types de ressources, fournissez la liste complète des types de ressources dans la commande, et pas uniquement les types de ressources que vous ajoutez. Vous pouvez avoir un maximum de 20 types de ressources dans une requête.

   Le *stack_identifier* est la pileARN, comme indiqué dans l'exemple de commande.

   ```
   $ aws resource-groups update-group-query \
       --group-name resource-group-name \
       --description "description" \
       --resource-query
    '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
   \"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
   \"resource_type2\"]}"}'
   ```

Voici un exemple de commande.

```
$ aws resource-groups update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

La commande renvoie la requête mise à jour comme résultat.

Événements du cycle de vie des groupes : surveillance des groupes de ressources pour détecter les modifications

Après AWS Resource Groups avoir organisé vos ressources en groupes, vous pouvez surveiller ces groupes pour détecter les modifications qui vous sont présentées sous forme d'événements. Vous pouvez recevoir une notification concernant un événement de groupe comme signal vous demandant de prendre des mesures. Par exemple, vous pouvez configurer une notification envoyée chaque fois que l'appartenance à un groupe change. Vous pouvez utiliser un événement lié à l'ajout d'un nouveau membre au groupe pour déclencher une fonction Lambda qui examine les modifications par programmation afin de s'assurer que les nouveaux membres du groupe répondent aux exigences de conformité définies par votre organisation. Une telle fonction Lambda pourrait effectuer une correction automatique pour tous les nouveaux membres du groupe qui ne répondent pas à ces exigences. Un événement provoqué par la suppression d'un membre du groupe peut déclencher une fonction Lambda qui effectue tout nettoyage requis, tel que la suppression de ressources liées.

En activant les événements du cycle de vie des groupes pour vos groupes de ressources, vous autorisez Amazon à capturer les événements relatifs aux modifications apportées à vos groupes EventBridge et à les mettre à la disposition de tous les différents services cibles EventBridge pris en charge. Vous pouvez ensuite configurer ces services cibles pour qu'ils prennent automatiquement les mesures requises par votre scénario. Ces cibles incluent une variété de AWS services tels qu'Amazon Simple Notification Service (AmazonSNS), Amazon Simple Queue Service (AmazonSQS) et AWS Lambda. Avec des services tels que Lambda, vos événements peuvent déclencher des réponses programmatiques qui utilisent du code pour effectuer les actions dont vous avez besoin. Pour obtenir la liste des AWS services que vous pouvez utiliser pour cibler EventBridge, consultez les EventBridge cibles Amazon dans le guide de EventBridge l'utilisateur Amazon.

Lorsque vous activez les événements du cycle de vie du groupe, AWS Resource Groups crée les éléments suivants :

- Rôle lié à un service AWS Identity and Access Management (IAM) autorisé à surveiller vos ressources pour détecter toute modification apportée à leurs balises et vos AWS CloudFormation piles pour détecter toute modification apportée aux ressources faisant partie d'une pile.
- Une EventBridge règle gérée par Resource Groups qui capture les détails de toute modification apportée aux balises ou aux piles de vos ressources. EventBridge utilise cette règle pour informer Resource Groups de ces modifications. Resource Groups génère ensuite des événements

d'adhésion auxquels vous pouvez EventBridge les envoyer pour que vos règles personnalisées puissent être traitées.

Le rôle lié au service ne peut être assumé que par le service Resource Groups. Pour plus d'informations sur le rôle lié à un service utilisé par Resource Groups pour cette fonctionnalité, consultez. Utilisation des rôles liés à un service pour les Resource Groups pour les groupes de ressources

Lorsque cette fonctionnalité est activée, Resource Groups génère un événement lorsque vous apportez l'une des modifications suivantes à un groupe de ressources :

- Créez un nouveau groupe de ressources.
- Mettez à jour la requête qui définit l'appartenance au groupe de ressources basé sur les requêtes.
- Mettez à jour la configuration d'un groupe de ressources lié à un service.
- Mettez à jour la description d'un groupe de ressources.
- Pour supprimer un groupe de ressources.
- Modifiez l'appartenance à un groupe de ressources en ajoutant ou en supprimant une ressource du groupe. Un changement d'adhésion peut également se produire lorsque les balises changent ou lorsqu'une AWS CloudFormation pile change.

> **Important**
>
> - Pour recevoir et répondre correctement aux événements de groupe, vous devez apporter des modifications à la fois à Resource Groups et EventBridge. Vous pouvez effectuer les modifications dans n'importe quel ordre, mais aucun événement de groupe n'est publié sur les EventBridge cibles tant que vous n'avez pas apporté de modifications aux deux services.
>
> - Les modifications apportées au groupe de ressources n'incluent pas les modifications apportées aux balises associées au groupe de ressources lui-même. Pour générer des événements en fonction des modifications de balises apportées à vos groupes, vous devez utiliser une EventBridge règle qui utilise la `aws.tag` source au lieu de la `aws.resource-groups` source. Pour plus d'informations, consultez la section Événements de changement de tag sur AWS Resources dans le guide de EventBridge l'utilisateur Amazon.

Rubriques

- Activation des événements du cycle de vie des groupes dans Resource Groups
- Création d'une EventBridge règle pour capturer les événements du cycle de vie du groupe et publier des notifications
- Désactiver les événements du cycle de vie des groupes
- Structure et syntaxe des événements du cycle de vie des Resource Groups

Activation des événements du cycle de vie des groupes dans Resource Groups

Pour recevoir des notifications concernant les modifications du cycle de vie de vos groupes de ressources, vous pouvez le faire sur les événements relatifs au cycle de vie des groupes. Resource Groups fournit ensuite des informations sur les modifications apportées par vos groupes à Amazon EventBridge. Dans EventBridge, vous pouvez évaluer les modifications et agir en conséquence à l'aide des règles que vous définissez dans le EventBridge service.

> **Autorisations minimales**
>
> Pour activer les événements du cycle de vie de groupe dans votre compte Compte AWS, vous devez vous connecter en tant que principal AWS Identity and Access Management (IAM) avec les autorisations suivantes :
>
> - `resource-groups:UpdateAccountSettings`
> - `iam:CreateServiceLinkedRole`
> - `events:PutRule`
> - `events:PutTargets`
> - `events:DescribeRule`
> - `events:ListTargetsByRule`
> - `cloudformation:DescribeStacks`
> - `cloudformation:ListStackResources`
> - `tag:GetResources`

Lorsque vous activez pour la première fois les événements du cycle de vie des groupes dans un Compte AWS, Resource Groups crée un rôle lié à un service nommé. `AWSServiceRoleForResourceGroups` Ce rôle géré est autorisé à utiliser une EventBridge règle gérée par Resource Groups. La règle surveille les balises associées à vos ressources et les AWS CloudFormation piles de votre compte pour détecter toute modification. Resource Groups publie ensuite ces modifications dans le bus d'événements par défaut sur Amazon EventBridge. Le service crée également une règle EventBridge gérée nommée`Managed.ResourceGroups.TagChangeEvents`. Cette règle enregistre les détails des modifications de balises de vos ressources. Cela permet à Resource Groups de générer des événements d'adhésion auxquels envoyer EventBridge pour que vos règles personnalisées puissent être traitées. Vos EventBridge règles peuvent ensuite répondre aux événements en envoyant des notifications aux cibles configurées par les règles.

Une fois ces étapes terminées, les règles qui recherchent ces événements devraient commencer à les recevoir dans quelques minutes.

Vous pouvez activer les événements du cycle de vie des groupes à l'aide de l'API du SDK AWS Management Console ou à l'aide d'une commande provenant de l'une AWS CLI ou de l'une des API du SDK.

> **Note**
>
> Vous ne pouvez pas activer les événements du cycle de vie des groupes si le quota de vos groupes de ressources est trop élevé. Pour plus d'informations, consultez la section Affichage des quotas de service.

AWS Management Console

Pour activer les événements du cycle de vie des groupes dans la console Resource Groups

1. Ouvrez la page Paramètres dans la console Resource Groups.
2. Dans la section Événements du cycle de vie du groupe, choisissez le commutateur situé à côté de Notifications désactivées.
3. Dans la boîte de dialogue de confirmation, choisissez Activer les notifications.

   Le commutateur de fonctionnalités affiche Les notifications sont activées.

Cela met fin à la première partie du processus. Après avoir activé les notifications d'événements, vous pouvez créer des règles dans Amazon EventBridge qui capturent les événements et les envoient à des destinataires spécifiques Services AWS pour traitement.

AWS CLI

Pour activer les événements du cycle de vie des groupes à l'aide du AWS CLI ou des AWS SDK

L'exemple suivant montre comment utiliser le AWS CLI pour activer les événements du cycle de vie des groupes dans Resource Groups. Entrez la commande avec le paramètre principal du service exactement comme indiqué. La sortie indique à la fois l'état actuel et l'état souhaité de la fonctionnalité.

```
$ aws resource-groups update-account-settings \
    --group-lifecycle-events-desired-status ACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "IN_PROGRESS"
    }
}
```

Vous pouvez vérifier que la fonctionnalité est activée en exécutant l'exemple de commande suivant. Lorsque les deux champs de statut affichent la même valeur, l'opération est terminée.

```
$ aws resource-groups get-account-settings
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "ACTIVE"
    }
}
```

Pour plus d'informations, consultez les ressources suivantes :

- AWS CLI — groupes de ressources aws update-account-settings et groupes de ressources aws get-account-settings
- API — UpdateAccountSettingset GetAccountSettings

Création d'une EventBridge règle pour capturer les événements du cycle de vie du groupe et publier des notifications

Vous pouvez activer les événements du cycle de vie des groupes pour vos groupes de ressources AWS Resource Groups afin de publier des événements sur Amazon EventBridge. Vous pouvez ensuite créer des EventBridge règles qui répondent à ces événements en les envoyant à d'autres Services AWS pour un traitement ultérieur.

AWS CLI

Le processus de création d'une règle EventBridge qui capture les événements et les envoie au service cible souhaité nécessite deux commandes CLI distinctes :

1. Créez la EventBridge règle pour capturer les événements souhaités
2. Associez à la EventBridge règle une cible capable de traiter les événements

Étape 1 : créer la EventBridge règle pour capturer les événements

L'AWS CLI`put-rule`exemple de commande suivant crée une EventBridge règle qui capture toutes les modifications des événements du cycle de vie de Resource Groups.

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
    --event-pattern '{"source":["aws.resource-groups"]}'
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchAllResourceGroupEvents"
}
```

La sortie inclut le Amazon Resource Name (ARN) de la nouvelle règle.

> **Note**
>
> Les valeurs de paramètres qui incluent des chaînes entre guillemets sont soumises à des règles de formatage différentes en fonction du système d'exploitation et du shell que vous utilisez. Pour les exemples présentés dans ce guide, nous montrons des commandes qui fonctionnent sur un shell Linux BASH. Pour obtenir des instructions sur le formatage de chaînes avec des guillemets intégrés pour d'autres systèmes

d'exploitation, tels que l'invite de commande Windows, voir Utilisation de guillemets dans les chaînes du Guide de AWS Command Line Interface l'utilisateur.
À mesure que les chaînes de paramètres deviennent plus complexes, il peut être plus facile et moins sujet aux erreurs d'accepter une valeur de paramètre dans un fichier texte au lieu de la saisir directement sur la ligne de commande.

Le modèle d'événements suivant limite les événements à ceux qui sont liés au groupe spécifié, identifié par son ARN. Ce modèle d'événement est une chaîne JSON complexe qui est beaucoup moins lisible lorsqu'elle est compressée en une chaîne JSON d'une seule ligne correctement échappée. Vous pouvez plutôt le stocker dans un fichier.

Stockez la chaîne JSON du modèle d'événement dans un fichier. Dans l'exemple de code suivant, le fichier est`eventpattern.txt`.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-resource-group-arn" ]
        }
    }
}
```

Exécutez ensuite la commande suivante pour créer la règle, en récupérant le modèle d'événement personnalisé dans le fichier.

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

Pour capturer d'autres types d'événements Resource Groups, remplacez la `--event-pattern` chaîne par des filtres tels que ceux présentés dans la sectionExemples de modèles d'événements EventBridge personnalisés pour différents cas d'utilisation.

Étape 2 : associer à la EventBridge règle une cible capable de traiter les événements

Maintenant que vous disposez d'une règle qui capture les événements qui vous intéressent, vous pouvez associer une ou plusieurs cibles pour effectuer un certain type de traitement sur les événements.

La AWS CLI `put-targets` commande suivante associe une rubrique Amazon Simple Notification Service (Amazon SNS) `my-sns-topic` nommée à la règle que vous avez créée dans l'exemple précédent. Tous les abonnés à la rubrique reçoivent une notification lorsqu'une modification est apportée au groupe spécifié dans la règle.

```
$ aws events put-targets \
    --rule CatchResourceGroupEventsForMyGroup \
    --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
    "FailedEntryCount": 0,
    "FailedEntries": []
}
```

À ce stade, toute modification de groupe correspondant au modèle d'événement de votre règle est automatiquement envoyée à la ou aux cibles configurées. Si, comme dans l'exemple précédent, la cible est un sujet Amazon SNS, tous les abonnés du sujet reçoivent un message contenant l'événement, comme décrit dans. Structure et syntaxe des événements du cycle de vie des Resource Groups

Pour plus d'informations, consultez les ressources suivantes :

- AWS CLI— aws events put-rule et aws events put-targets
- API — PutRuleet PutTargets

Création d'une règle pour capturer uniquement des types d'événements spécifiques du cycle de vie d'un groupe

Vous pouvez créer une règle avec un modèle d'événement personnalisé qui capture uniquement les événements qui vous intéressent. Pour plus de détails sur la manière de filtrer les événements entrants à l'aide d'un modèle d'événement personnalisé, consultez les EventBridge événements Amazon dans le guide de EventBridge l'utilisateur Amazon.

Supposons, par exemple, que vous souhaitiez qu'une règle traite uniquement les notifications Resource Groups indiquant la création d'un nouveau groupe de ressources. Vous pouvez utiliser un modèle d'événement personnalisé similaire à l'exemple suivant.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change" ],
    "detail": {
        "state-change": "create"
    }
}
```

Ce filtre capture uniquement les événements dont les valeurs exactes figurent dans les champs spécifiés. Pour obtenir la liste complète des champs que vous pouvez associer, consultezStructure et syntaxe des événements du cycle de vie des Resource Groups.

Désactiver les événements du cycle de vie des groupes

Vous pouvez désactiver les événements du cycle de vie des groupes pour arrêterAWS Resource Groups de transmettre des événements à Amazon EventBridge. Vous pouvez le faire avec laAWS Management Console ou à l'aide d'une commande de l'AWS CLIou de l'une des API du SDK.

> **Note**
>
> La désactivation des événements du cycle de vie des groupes entraîne la suppression de la EventBridge règle gérée des Resource Groups utilisée pour analyser les balises et lesAWS CloudFormation piles de ressources afin de détecter les modifications. Les Resource Groups ne peuvent plus transmettre ces modifications à EventBridge. Toutes les règles que vous avez définies dans EventBridge ce document qui recherchent des événements de Resource Groups cessent de recevoir des événements à traiter. Si vous avez l'intention de réactiver les événements du cycle de vie des groupes à l'future, vous pouvez désactiver vos règles. Si vous n'avez pas l'intention d'utiliser à nouveau ces règles, vous pouvez les supprimer. Pour plus d'informations, consultez la section Désactivation ou suppression d'une EventBridge règle dans le Guide de EventBridge l'utilisateur Amazon.
>
> La désactivation des événements du cycle de vie du groupe ne supprime pas le rôle lié au service. Vous pouvez supprimer le rôle lié à un service à l'aide d'IAM. Si vous devez réactiver ultérieurement les événements du cycle de vie des groupes et que le rôle lié au service n'existe pas, Resource Groups le recrée automatiquement.

Autorisations minimales

Pour désactiver les événements du cycle de vie de groupe dans votre compte actuelCompte AWS, vous devez vous connecter en tant que principalAWS Identity and Access Management (IAM) avec les autorisations suivantes :

- `resource-groups:UpdateAccountSettings`
- `events:DeleteRule`
- `events:RemoveTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`

AWS Management Console

Pour désactiver les notifications d'événements liés au cycle de vie des groupes à EventBridge

1. Ouvrez la page Paramètres dans la console Resource Groups.
2. Dans la section Événements du cycle de vie du groupe, sélectionnez le commutateur situé à côté de Notifications sont activées.
3. Dans la boîte de dialogue de confirmation, choisissez Désactiver les notifications.

   Le commutateur de fonctionnalité s'affiche : les notifications d'événements sont désactivées.

À ce stade, les Resource Groups n'envoient plus d'événements au bus d'événements EventBridge par défaut, ni les règles que vous ne recevez plus d'événements de notification de groupe à traiter. Vous pouvez éventuellement supprimer ces règles pour terminer le nettoyage.

AWS CLI

Pour désactiver les notifications d'événements liés au cycle de vie des groupes à EventBridge

L'exemple suivant montre comment utiliser leAWS CLI pour désactiver les événements du cycle de vie des groupes dans les Resource Groups.

```
$ aws resource-groups update-account-settings \
    ----group-lifecycle-events-desired-status INACTIVE
{
```

```
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "INACTIVE",
        "GroupLifecycleEventsStatus": "INACTIVE"
    }
}
```

Pour plus d'informations, consultez les ressources suivantes :

- AWS CLI— groupes de ressources AWS update-account-settings et groupes de ressources AWS get-account-settings
- API — UpdateAccountSettingset GetAccountSettings

Structure et syntaxe des événements du cycle de vie des Resource Groups

Rubriques

- Structure du detail champ
- Exemples de modèles d'événements EventBridge personnalisés pour différents cas d'utilisation

Les événements du cycle de vie de AWS Resource Groups prennent la forme de chaînes d'JSONobjets au format général suivant.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group ... Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
    ],
    "detail": {
        ...
    }
}
```

Pour en savoir plus sur les champs communs à tous les EventBridge événements Amazon, consultez les EventBridge événements Amazon dans le guide de EventBridge l'utilisateur Amazon. Les détails spécifiques à Resource Groups sont expliqués dans le tableau suivant.

Nom de champ	Type	Description
`detail-type`	Chaîne	Pour Resource Groups, le `detail-type` champ est toujours l'une des valeurs suivantes : • `ResourceGroups Group State Change` — Représente les modifications apportées à l'état général du groupe et à ses propriétés. • `ResourceGroups Group Membership Change` — Représente les modifications apportées à l'appartenance au groupe.
`source`	Chaîne	Pour Resource Groups, cette valeur est toujours`"aws.resource-groups"` .
`resources`	Un tableau de noms de ressources Amazon (ARNs)	Ce champ inclut toujours le nom de ressource Amazon (ARN) du groupe avec la modification qui a déclenché cet événement. Ce champ peut également inclure ARNs les ressources ajoutées ou supprimées du groupe, le cas échéant.
`detail`	JSONchaîne d'objets	Il s'agit de la charge utile de l'événement. Le contenu du `detail` champ varie en fonction de la valeur du`detail-type` . Consultez la section suivante pour plus d'informations.

Structure du **`detail`** champ

Le `detail` champ inclut tous les détails spécifiques au service Resource Groups concernant une modification spécifique. Le `detail` champ peut prendre l'une des deux formes suivantes : un

changement d'état de groupe ou un changement d'adhésion, en fonction de la valeur du `detail-type` champ décrit dans la section précédente.

> **Important**
>
> Lors de ces événements, les groupes de ressources sont identifiés par une combinaison du groupe ARN et d'un `"unique-id"` champ contenant un UUID. En incluant un élément dans l'identité d'un groupe de ressources, vous pouvez faire la distinction entre un groupe supprimé et un autre groupe créé ultérieurement UUID sous le même nom. Nous vous recommandons de traiter une concaténation de l'identifiant unique ARN et comme clé pour le groupe de vos programmes qui interagit avec ces événements.

Modification de l'état du groupe

`"detail-type": "ResourceGroups Group State Change"`

Cette `detail-type` valeur indique que l'état du groupe lui-même, y compris ses métadonnées, a changé. Cette modification se produit lorsqu'un groupe est créé, mis à jour ou supprimé, comme indiqué dans le `"change"` champ du`detail`.

Les informations incluses dans la `details` section lorsque cela `detail-type` est spécifié incluent les champs décrits dans le tableau suivant.

Nom de champ	Type	Description
`event-sequence`	Double	Nombre croissant de façon monotone qui indique la séquence des événements pour un groupe spécifique. Le numéro est réinitialisé lorsque vous supprimez le groupe et que vous créez un autre groupe portant le même nom.
`group`	`Group`JSONobjet	L'objet de groupe associé à l'événement par son ARN nom et son identifiant unique.
`state-change`	Chaîne	Type de changement d'état qui s'est produit. Il peut s'agir de l'une des valeurs suivantes : • `create`

Nom de champ	Type	Description
		• update • delete
old-state	GroupState JSONobjet	État du groupe avant la modification. L'objet inclut uniquement les valeurs des propriétés modifiées.
new-state	GroupState JSONobjet	État du groupe après la modification. L'objet inclut uniquement les valeurs des propriétés modifiées.

L'groupJSONobjet contient les éléments décrits dans le tableau suivant.

Nom de champ	Type	Description
arn	Chaîne	Celui ARN du groupe.
name	Chaîne	Le nom convivial du groupe.
unique-id	GUID	Une GUID valeur unique qui fait la distinction entre un groupe supprimé et un autre groupe créé ultérieurement avec le même nom etARN. Utilisez la concaténation de ARN et cette valeur comme clé unique pour le groupe lorsque vous consommez ces événements dans votre code.

Les GroupState JSON objets contiennent les éléments décrits dans le tableau suivant.

Nom de champ	Type	Description
description	Chaîne	Description du groupe de ressources fournie par le client.
resource-query	ResourceQuery JSONobjet	Une JSON représentation de la requête qui définit les membres du groupe. Ce champ n'est présent que pour les groupes basés sur une requête. La syntaxe de ce champ est définie par le type de

Nom de champ	Type	Description
		ResourceQuery API données. Des exemples de cela sont inclus dans les exemples d'événements de création et de mise à jour.
`group-configuration`	`Configuration` JSONobjet	JSONReprésentation des paramètres de configuration associés à un groupe lié à un service. Pour plus d'informations, consultez la section Configurations de service pour les groupes de ressources dans la AWS Resource Groups APIréférence.

Chacun des exemples de code suivants illustre le contenu du `detail` champ pour chaque `state-change` type.

Création

`"state-change": "create"`

L'événement indique qu'un nouveau groupe a été créé. L'événement contient toutes les propriétés de métadonnées du groupe définies lors de la création du groupe. Cet événement est généralement suivi d'un ou de plusieurs événements d'adhésion à un groupe, sauf si le groupe est vide. Les propriétés dont la valeur est nulle ne sont pas affichées dans le corps de l'événement.

L'exemple d'événement suivant indique un groupe de ressources nouvellement créé nommé`my-service-group`. Dans cet exemple, le groupe utilise une requête basée sur des balises qui correspond uniquement aux instances Amazon Elastic Compute Cloud (AmazonEC2) qui possèdent la balise`"project"="my-service"`.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
```

```
    "detail": {
        "event-sequence": 1.0,
        "state-change": "create",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service-group",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Mettre à jour

`"state-change": "update"`

L'événement indique qu'un groupe existant a été modifié d'une manière ou d'une autre. L'événement ne contient que les propriétés modifiées par rapport à l'état précédent. Les propriétés qui n'ont pas été modifiées ne sont pas affichées dans le corps de l'événement.

L'exemple d'événement suivant indique que la requête basée sur des balises dans le groupe de ressources de l'exemple précédent a été modifiée pour inclure également les ressources EC2 du volume Amazon dans le groupe.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
```

```
    ],
    "detail": {
        "event-sequence": 3.0,
        "state-change": "update",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
 \"AWS::EC2::Volume\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        },
        "old-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"Project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Suppression

`"state-change": "delete"`

L'événement indique qu'un groupe existant a été supprimé. Le champ de détail ne contient aucune métadonnée concernant le groupe autre que son identification. Le `event-sequence` champ est réinitialisé après cet événement car il s'agit, par définition, du dernier événement pour cet événement `arn` et`unique-id`.

```
{
    "version": "0",
```

```
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
    ],
    "detail": {
        "event-sequence": 4.0,
        "state-change": "delete",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        }
    }
}
```

Modification de l'adhésion au groupe

`"detail-type": "ResourceGroups Group Membership Change"`

Cette `detail-type` valeur indique que l'appartenance au groupe a été modifiée par l'ajout ou la suppression d'une ressource au groupe. Lorsque cela `detail-type` est spécifié, le `resources` champ ARN de niveau supérieur inclut le groupe dont les membres ont été modifiés et les ARNs ressources qui ont été ajoutées ou supprimées du groupe.

Les informations incluses dans la `details` section lorsque cela `detail-type` est spécifié incluent les champs décrits dans le tableau suivant.

Nom de champ	Type	Description
`event-sequence`	Double	Nombre croissant de façon monotone qui indique la séquence des événements pour un groupe spécifique. Le numéro est réinitialisé lorsque le groupe est supprimé et que son identifiant unique change.

Nom de champ	Type	Description
`group`	`Group`JSONobjet	Identifie l'objet de groupe associé à l'événement par son ARN nom et son identifiant unique.
`resources`	Tableau d'`ResourceChange` JSONobjets	Un ensemble de ressources dont l'appartenance au groupe a changé. Cet `ResourceChange` objet contient les champs suivants pour chaque ressource : • `membership-change` — La valeur est `"add"` soit`"remove"`. • `arn`— Le ARN nom de la ressource ajoutée ou supprimée. • `resource-type` — Type de ressource ajoutée ou supprimée.

L'exemple de code suivant illustre le contenu de l'événement pour un type de changement d'adhésion typique. Cet exemple montre qu'une ressource est ajoutée au groupe et qu'une ressource est supprimée du groupe.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group Membership Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
    ],
    "detail": {
        "event-sequence": 2.0,
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
```

```
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "resources": [
            {
                "membership-change": "add",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
                "resource-type": "AWS::EC2::Instance"
            },
            {
                "membership-change": "remove",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
                "resource-type": "AWS::EC2::Instance"
            }
        ]
    }
}
```

Exemples de modèles d'événements EventBridge personnalisés pour différents cas d'utilisation

Les exemples de modèles d'événements EventBridge personnalisés suivants filtrent les événements générés par Resource Groups uniquement en fonction de ceux qui vous intéressent pour une règle et une cible d'événement spécifiques.

Dans les exemples de code suivants, si un groupe ou une ressource spécifique est nécessaire, remplacez chaque *`user input placeholder`* avec vos propres informations.

Tous les événements Resource Groups

```
{
    "source": [ "aws.resource-groups" ]
}
```

Événements relatifs à l'état du groupe ou à la modification des membres

L'exemple de code suivant concerne tous les changements d'état du groupe.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change " ]
```

```
}
```

L'exemple de code suivant concerne toutes les modifications apportées à l'appartenance à un groupe.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ]
}
```

Événements pour un groupe spécifique

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-group-arn" ]
        }
    }
}
```

L'exemple précédent capture les modifications apportées au groupe spécifié. L'exemple suivant fait de même et capture également les modifications lorsque le groupe est une ressource membre d'un autre groupe.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [ "my-group-arn" ]
}
```

Événements relatifs à une ressource spécifique

Vous ne pouvez filtrer que les événements de modification de l'appartenance à un groupe pour des ressources spécifiques aux membres.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change " ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

Événements relatifs à un type de ressource spécifique

Vous pouvez utiliser le préfixe correspondant à ARNs pour faire correspondre les événements d'un type de ressource spécifique.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [
        { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
    ]
}
```

Vous pouvez également utiliser une correspondance exacte en utilisant des `resource-type` identifiants, ce qui peut permettre de faire correspondre de manière concise plusieurs types. Contrairement à l'exemple précédent, l'exemple suivant ne correspond qu'aux événements de changement d'appartenance à un groupe, car les événements de changement d'état du groupe n'incluent `resources` aucun champ dans leur `detail` champ.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "resources": {
                "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
         }
    }
}
```

Tous les événements de suppression de ressources

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
        }
    }
}
```

Tous les événements de suppression de ressources pour une ressource spécifique

```
 {
```

```
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ],
                "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
         }
    }
}
```

Vous ne pouvez pas utiliser le `resources` tableau de niveau supérieur utilisé dans le premier exemple de cette section pour ce type de filtrage d'événements. En effet, une ressource de l'`resources`élément de niveau supérieur peut être une ressource ajoutée à un groupe et l'événement correspondra toujours. En d'autres termes, l'exemple de code suivant peut renvoyer des événements inattendus. Utilisez plutôt la syntaxe indiquée dans l'exemple précédent.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
         }
     }
}
```

Supprimer des groupes de ressources de AWS Resource Groups

Vous pouvez utiliser la AWS Resource Groups console ou le AWS CLI pour supprimer des groupes de ressources AWS Resource Groups. La suppression d'un groupe de ressources ne supprime pas les ressources membres du groupe ou les balises sur les ressources membres. Elle supprime uniquement la structure du groupe et les balises au niveau du groupe.

Console

Pour supprimer des groupes de ressources

1. Connectez-vous à la console AWS Resource Groups.
2. Dans le volet de navigation, sélectionnez Saved Resource Groups.
3. Choisissez le nom du groupe de ressources que vous souhaitez supprimer, puis choisissez Afficher les détails.
4. Sur la page détaillée du groupe, choisissez Supprimer dans le coin supérieur droit.
5. Lorsque vous êtes invité à confirmer la suppression, choisissez Delete (Supprimer).

AWS CLI & AWS SDKs

Pour supprimer des groupes de ressources

1. Exécutez la commande suivante en remplaçant *resource_group_name* avec le nom de votre groupe.

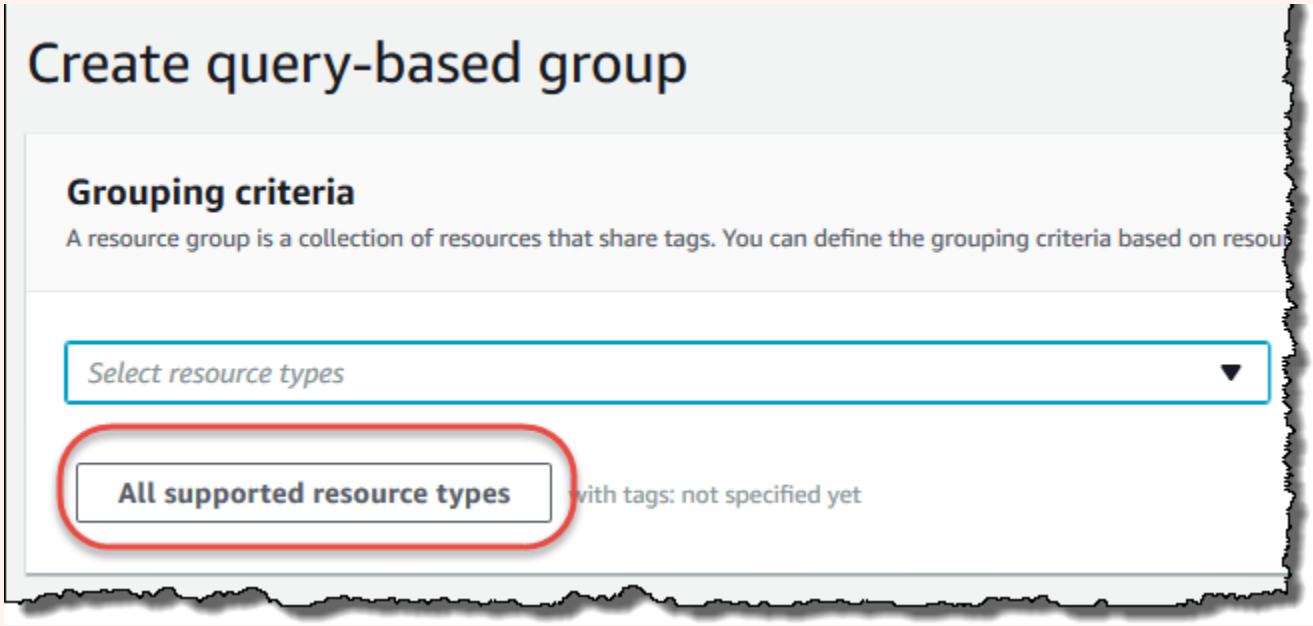
```
$ aws resource-groups delete-group \
    --group-name resource_group_name
```

2. Lorsque vous êtes invité à confirmer la suppression, saisissez `yes`, puis appuyez sur Enter (Entrée).

Types de ressources que vous pouvez utiliser avec AWS Resource Groups l'éditeur de balises

Vous pouvez utiliser le AWS Management Console ou le AWS CLI pour créer des groupes de ressources, puis interagir avec les ressources des membres par le biais de ces groupes. Vous pouvez ajouter des balises à de nombreuses AWS ressources, puis utiliser ces balises pour gérer l'appartenance à un groupe. Cette rubrique décrit les types de AWS ressources que vous pouvez inclure dans les groupes de ressources en utilisant AWS Resource Groups, ainsi que les types de ressources que vous pouvez baliser à l'aide de l'éditeur de balises.

> **Important**
>
> Un groupe de ressources basé sur une requête pour Tous les types de ressources pris en charge peut ajouter des membres automatiquement au fil du temps, car les nouvelles ressources sont prises en charge par Resource Groups. Lorsque vous exécutez des automatisations ou d'autres tâches groupées sur un groupe de ressources existant en fonction de tous les types de ressources pris en charge, sachez que les actions peuvent s'exécuter sur bien plus de ressources que celles du groupe lorsque vous l'avez créé pour la première fois. Cela peut également signifier que les automatisations ou les tâches que vous avez créées pour d'autres ressources sont appliquées à des ressources éventuellement inattendues ou à des ressources sur lesquelles les tâches ne peuvent pas être effectuées correctement. Dans ces cas, vous pouvez ajouter un filtre de type de ressource pour spécifier que seules les ressources des types spécifiés peuvent faire partie du groupe.



Les tableaux suivants répertorient les types de ressources pris en charge pour le balisage dans l'éditeur de balises, pour l'adhésion à des groupes basés sur des requêtes de balises et pour l'adhésion à AWS CloudFormation des groupes basés sur des piles.

Définitions de colonnes

- Balisage de l'éditeur de balises : vous pouvez baliser les ressources de ce type à l'aide de la console de l'éditeur de balises. Dans le cas contraire, vous devez utiliser les services de balisage pris en charge de manière native par le service propriétaire de cette ressource AWS Resource Groups Tagging APIou les services de balisage pris en charge de manière native.
- Groupes basés sur des balises : vous pouvez inclure des ressources de ce type dans des groupes de ressources dont l'appartenance est déterminée par les balises associées aux ressources. Le groupe spécifie les noms et les valeurs des clés de balise, et toutes les ressources dont les balises correspondent font automatiquement partie du groupe.
- AWS CloudFormation Groupes basés sur des piles : vous pouvez inclure des ressources de ce type dans des groupes de ressources dont les membres sont les ressources créées dans le cadre d'une CloudFormation pile. Le groupe spécifie l'ARN de la pile, et toutes ses ressources sont automatiquement membres du groupe. L'ajout de balises à une AWS CloudFormation pile entraîne une mise à jour de la pile.

Pour obtenir la liste des types de ressources déconseillés et qui ne sont plus pris en charge par Resource Groups, consultez la section Types de ressources déconseillés à la fin de cette rubrique.

> **Note**
>
> Resource Groups et Tag Editor prennent en charge les types de ressources présentés dans le tableau suivant, mais certains types de ressources peuvent ne pas être disponibles dans votre Région AWS.

Amazon API Gateway

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ApiGateway::Account`	✗ Non	✗ Non	✓ Oui
`AWS::ApiGateway::ApiKey`	✗ Non	✓ Oui	✓ Oui
`AWS::ApiGateway::ClientCertificate`	✗ Non	✓ Oui	✗ Non
`AWS::ApiGateway::DomainName`	✗ Non	✗ Non	✓ Oui
`AWS::ApiGateway::RestApi`	✗ Non	✓ Oui	✓ Oui
`AWS::ApiGateway::Stage`	✗ Non	✓ Oui	✗ Non
`AWS::ApiGateway::UsagePlan`	✗ Non	✓ Oui	✓ Oui

Amazon API Gateway V2

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ApiGatewayV2::Api`	✗ Non	✓ Oui	✗ Non

IAM Access Analyzer

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::AccessAnalyzer::Analyzer`	✗ Non	✓ Oui	✗ Non

AWS Amplify

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Amplify::App`	✗ Non	✓ Oui	✗ Non

AWS App Mesh

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::AppMesh::Mesh`	✗ Non	✓ Oui	✗ Non

Amazon AppStream

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::AppStream::AppBlock`	✗ Non	✓ Oui	✗ Non
`AWS::AppStream::Application`	✗ Non	✓ Oui	✗ Non
`AWS::AppStream::Fleet`	✓ Oui	✓ Oui	✓ Oui
`AWS::AppStream::ImageBuilder`	✓ Oui	✓ Oui	✓ Oui
`AWS::AppStream::Stack`	✓ Oui	✓ Oui	✓ Oui

AWS AppSync

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::AppSync::DataSource`	✕ Non	✕ Non	✓ Oui
`AWS::AppSync::GraphQLApi`	✕ Non	✕ Non	✓ Oui

Amazon Athena

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Athena::DataCatalog`	✕ Non	✓ Oui	✕ Non
`AWS::Athena::WorkGroup`	✕ Non	✓ Oui	✕ Non

AWS Backup

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Backup::BackupPlan`	✕ Non	✓ Oui	✕ Non
`AWS::Backup::BackupVault`	✕ Non	✓ Oui	✕ Non
`AWS::Backup::ReportPlan`	✕ Non	✓ Oui	✕ Non

AWS Batch

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Batch::ComputeEnvironment`	✕ Non	✓ Oui	✕ Non
`AWS::Batch::JobQueue`	✕ Non	✓ Oui	✕ Non
`AWS::Batch::SchedulingPolicy`	✕ Non	✓ Oui	✕ Non

AWS Billing Conductor

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::BillingConductor::BillingGroup`	✕ Non	✓ Oui	✓ Oui
`AWS::BillingConductor::CustomLineItem`	✕ Non	✓ Oui	✓ Oui
`AWS::BillingConductor::PricingPlan`	✕ Non	✓ Oui	✓ Oui
`AWS::BillingConductor::PricingRule`	✕ Non	✓ Oui	✓ Oui

Amazon Braket

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Braket::Job`	✕ Non	✓ Oui	✕ Non
`AWS::Braket::QuantumTask`	✓ Oui	✓ Oui	✕ Non

AWS Certificate Manager

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CertificateManager::Certificate`	✓ Oui	✓ Oui	✓ Oui

AWS Certificate Manager Autorité de certification privée

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ACMPCA::CertificateAuthority`	× Non	✓ Oui	× Non

AWS Cloud9

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Cloud9::Environment`	✓ Oui	✓ Oui	× Non

AWS CloudFormation

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CloudFormation::Stack`	✓ Oui	✓ Oui	✓ Oui

Amazon CloudFront

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CloudFront::Distribution`	✓ Oui[1]	✓ Oui[2]	✓ Oui[2]
`AWS::CloudFront::StreamingDistribution`	✓ Oui[1]	✓ Oui[2]	✓ Oui[2]

[1] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Pour utiliser l'éditeur de balises afin de créer ou de modifier des balises pour ce type `us-east-1` de ressource, vous devez les inclure dans la liste Sélectionner les régions sous Rechercher les ressources à étiqueter dans la console de l'éditeur de balises.

[2] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Les Resource Groups étant gérés séparément pour chaque région, vous devez passer AWS Management Console à celui Région AWS qui contient les ressources que vous souhaitez inclure dans le groupe. Pour créer un groupe de ressources contenant une ressource globale, vous devez

configurer votre US-east-1 AWS Management Console à l'aide du sélecteur de région situé dans le coin supérieur droit du. AWS Management Console

AWS Cloud Map

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ServiceDiscovery::Service`	✕ Non	✓ Oui	✕ Non

AWS CloudTrail

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CloudTrail::Channel`	✕ Non	✓ Oui	✕ Non
`AWS::CloudTrail::EventDataStore`	✕ Non	✓ Oui	✕ Non
`AWS::CloudTrail::Trail`	✓ Oui	✓ Oui	✓ Oui

Amazon CloudWatch

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CloudWatch::Alarm`	✓ Oui	✓ Oui	✓ Oui
`AWS::CloudWatch::Dashboard`	× Non	× Non	✓ Oui
`AWS::CloudWatch::InsightRule`	× Non	✓ Oui	× Non
`AWS::CloudWatch::MetricStream`	× Non	✓ Oui	× Non
`AWS::CloudWatch::ServiceLevelObjective`	× Non	✓ Oui	× Non

Amazon CloudWatch Logs

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Logs::Destination`	× Non	✓ Oui	× Non
`AWS::Logs::LogGroup`	× Non	✓ Oui	✓ Oui

Amazon CloudWatch Synthetics

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Synthetics::Canary`	✗ Non	✓ Oui	✓ Oui

AWS CodeArtifact

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeArtifact::Domain`	✓ Oui	✓ Oui	✓ Oui
`AWS::CodeArtifact::Repository`	✓ Oui	✓ Oui	✓ Oui

AWS CodeBuild

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeBuild::Project`	✓ Oui	✓ Oui	✗ Non

AWS CodeCommit

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeCommit::Repository`	✓ Oui	✓ Oui	× Non

AWS CodeDeploy

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeDeploy::Application`	× Non	✓ Oui	✓ Oui
`AWS::CodeDeploy::DeploymentConfig`	× Non	× Non	✓ Oui

CodeGuru Réviseur Amazon

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeGuruReviewer::RepositoryAssociation`	✓ Oui	✓ Oui	✓ Oui

Amazon CodeGuru Profiler

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeGuruProfiler::ProfilingGroup`	× Non	✓ Oui	× Non

AWS CodePipeline

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodePipeline::CustomActionType`	× Non	✓ Oui	× Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodePipeline::Pipeline`	✓ Oui	✓ Oui	✓ Oui
`AWS::CodePipeline::Webhook`	✓ Oui	✓ Oui	✓ Oui

AWS CodeConnections

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::CodeStarConnections::Connection`	× Non	✓ Oui	× Non

Amazon Cognito

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Cognito::IdentityPool`	✓ Oui	✓ Oui	✓ Oui
`AWS::Cognito::UserPool`	✓ Oui	✓ Oui	✓ Oui

Amazon Comprehend

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Comprehend::DocumentClassifier`	✓ Oui	✓ Oui	× Non
`AWS::Comprehend::EntityRecognizer`	✓ Oui	✓ Oui	× Non

AWS Config

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Config::AggregationAuthorization`	× Non	✓ Oui	× Non
`AWS::Config::ConfigRule`	✓ Oui	✓ Oui	× Non
`AWS::Config::ConfigurationAggregator`	× Non	✓ Oui	× Non
`AWS::Config::StoredQuery`	× Non	✓ Oui	× Non

Amazon Connect

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Connect::Instance`	✕ Non	✓ Oui	✕ Non
`AWS::Connect::PhoneNumber`	✕ Non	✓ Oui	✕ Non

Amazon Connect Wisdom

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Wisdom::Assistant`	✕ Non	✓ Oui	✓ Oui
`AWS::Wisdom::AssistantAssociation`	✕ Non	✓ Oui	✓ Oui
`AWS::Wisdom::Content`	✕ Non	✓ Oui	✕ Non
`AWS::Wisdom::KnowledgeBase`	✕ Non	✓ Oui	✓ Oui
`AWS::Wisdom::Session`	✕ Non	✓ Oui	✕ Non

AWS Data Exchange

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DataExchange::DataSet`	✓ Oui	✓ Oui	× Non
`AWS::DataExchange::Revision`	× Non	✓ Oui	× Non

AWS Data Pipeline

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DataPipeline::Pipeline`	✓ Oui	✓ Oui	✓ Oui

AWS DataSync

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DataSync::Task`	× Non	✓ Oui	× Non

AWS Database Migration Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DMS::Certificate`	✓ Oui	✓ Oui	× Non
`AWS::DMS::Endpoint`	✓ Oui	✓ Oui	✓ Oui
`AWS::DMS::EventSubscription`	✓ Oui	✓ Oui	× Non
`AWS::DMS::ReplicationInstance`	✓ Oui	✓ Oui	✓ Oui
`AWS::DMS::ReplicationSubnetGroup`	✓ Oui	✓ Oui	× Non
`AWS::DMS::ReplicationTask`	✓ Oui	✓ Oui	× Non

AWS Device Farm

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DeviceFarm::InstanceProfile`	× Non	✓ Oui	× Non
`AWS::DeviceFarm::Project`	× Non	✓ Oui	× Non
`AWS::DeviceFarm::TestGridProject`	× Non	✓ Oui	× Non

Amazon DynamoDB

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DynamoDB::Table`	✓ Oui	✓ Oui	✓ Oui

Amazon EMR

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EMR::Cluster`	✓ Oui	✓ Oui	✓ Oui

Conteneurs Amazon EMR

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EMRContainers::JobRun`	× Non	✓ Oui	× Non
`AWS::EMRContainers::VirtualCluster`	✓ Oui	✓ Oui	✓ Oui

Amazon EMR sans serveur

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EMRServerless::Application`	✗ Non	✓ Oui	✓ Oui
`AWS::EMRServerless::JobRun`	✗ Non	✓ Oui	✗ Non

Amazon ElastiCache

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ElastiCache::CacheCluster`	✓ Oui	✓ Oui	✓ Oui
`AWS::ElastiCache::ParameterGroup`	✗ Non	✓ Oui	✗ Non
`AWS::ElastiCache::SecurityGroup`	✗ Non	✓ Oui	✗ Non
`AWS::ElastiCache::Snapshot`	✓ Oui	✓ Oui	✗ Non
`AWS::ElastiCache::SubnetGroup`	✗ Non	✓ Oui	✗ Non
`AWS::ElastiCache::User`	✗ Non	✓ Oui	✗ Non
`AWS::ElastiCache::UserGroup`	✗ Non	✓ Oui	✗ Non

AWS Elastic Beanstalk

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ElasticBeanstalk::Application`	✓ Oui	✓ Oui	× Non
`AWS::ElasticBeanstalk::ApplicationVersion`	× Non	✓ Oui	× Non
`AWS::ElasticBeanstalk::ConfigurationTemplate`	× Non	✓ Oui	× Non
`AWS::ElasticBeanstalk::Environment`	× Non	✓ Oui	× Non

Amazon Elastic Compute Cloud (Amazon EC2)

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EC2::CapacityReservation`	× Non	✓ Oui	× Non
`AWS::EC2::CapacityReservationFleet`	× Non	✓ Oui	× Non
`AWS::EC2::CarrierGateway`	× Non	✓ Oui	× Non
`AWS::EC2::ClientVpnEndpoint`	× Non	✓ Oui	× Non
`AWS::EC2::CoipPool`	× Non	✓ Oui	× Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EC2::CustomerGateway`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::DHCPOptions`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::EC2Fleet`	× Non	✓ Oui	× Non
`AWS::EC2::EgressOnlyInternetGateway`	× Non	✓ Oui	× Non
`AWS::EC2::EIP`	✓ Oui	✓ Oui	× Non
`AWS::EC2::ExportImageTask`	× Non	✓ Oui	× Non
`AWS::EC2::ExportInstanceTask`	× Non	✓ Oui	× Non
`AWS::EC2::FlowLog`	× Non	✓ Oui	× Non
`AWS::EC2::FpgaImage`	× Non	✓ Oui	× Non
`AWS::EC2::Host`	× Non	✓ Oui	× Non
`AWS::EC2::HostReservation`	× Non	✓ Oui	× Non
`AWS::EC2::Image`	✓ Oui	✓ Oui	× Non
`AWS::EC2::ImportImageTask`	× Non	✓ Oui	× Non
`AWS::EC2::ImportSnapshotTask`	× Non	✓ Oui	× Non
`AWS::EC2::Instance`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::InstanceEventWindow`	× Non	✓ Oui	× Non
`AWS::EC2::InternetGateway`	✓ Oui	✓ Oui	✓ Oui

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EC2::IPv4Pool`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::IPv6Pool`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::KeyPair`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::LaunchTemplate`	✗ Non	✓ Oui	✓ Oui
`AWS::EC2::LocalGateway`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::LocalGatewayRouteTable`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::LocalGatewayRouteTableVPCAssociation`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::LocalGatewayVirtualInterface`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::LocalGatewayVirtualInterfaceGroup`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::NatGateway`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::NetworkAcl`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::NetworkInsightsAccessScope`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	✗ Non	✓ Oui	✗ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EC2::NetworkInsightsAnalysis`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::NetworkInsightsPath`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::NetworkInterface`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::PlacementGroup`	✗ Non	✓ Oui	✓ Oui
`AWS::EC2::PrefixList`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::ReplaceRootVolumeTask`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::ReservedInstance`	✓ Oui	✓ Oui	✗ Non
`AWS::EC2::RouteTable`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::SecurityGroup`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::Snapshot`	✓ Oui	✓ Oui	✗ Non
`AWS::EC2::SpotFleet`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::SpotInstanceRequest`	✓ Oui	✓ Oui	✗ Non
`AWS::EC2::Subnet`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::SubnetCidrReservation`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::TrafficMirrorFilter`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::TrafficMirrorSession`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::TrafficMirrorTarget`	✗ Non	✓ Oui	✗ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
AWS::EC2::TransitGateway	✗ Non	✓ Oui	✗ Non
AWS::EC2::TransitGatewayAttachment	✗ Non	✓ Oui	✗ Non
AWS::EC2::TransitGatewayConnectPeer	✗ Non	✓ Oui	✗ Non
AWS::EC2::TransitGatewayMulticastDomain	✗ Non	✓ Oui	✗ Non
AWS::EC2::TransitGatewayPolicyTable	✗ Non	✓ Oui	✗ Non
AWS::EC2::TransitGatewayRouteTable	✗ Non	✓ Oui	✗ Non
AWS::EC2::TransitGatewayRouteTableAnnouncement	✗ Non	✓ Oui	✗ Non
AWS::EC2::VerifiedAccessEndpoint	✗ Non	✓ Oui	✗ Non
AWS::EC2::VerifiedAccessGroup	✗ Non	✓ Oui	✗ Non
AWS::EC2::VerifiedAccessInstance	✗ Non	✓ Oui	✗ Non
AWS::EC2::VerifiedAccessTrustProvider	✗ Non	✓ Oui	✗ Non
AWS::EC2::Volume	✓ Oui	✓ Oui	✓ Oui
AWS::EC2::VPC	✓ Oui	✓ Oui	✓ Oui
AWS::EC2::VPCEndpoint	✗ Non	✓ Oui	✗ Non
AWS::EC2::VPCEndpointConnection	✗ Non	✓ Oui	✗ Non
AWS::EC2::VPCEndpointService	✗ Non	✓ Oui	✗ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EC2::VPCEndpointServicePermissions`	✗ Non	✓ Oui	✗ Non
`AWS::EC2::VPCPeeringConnection`	✗ Non	✓ Oui	✓ Oui
`AWS::EC2::VPNConnection`	✓ Oui	✓ Oui	✓ Oui
`AWS::EC2::VPNGateway`	✓ Oui	✓ Oui	✓ Oui

Amazon Elastic Container Registry

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ECR::Repository`	✗ Non	✓ Oui	✗ Non

Amazon Elastic Container Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ECS::CapacityProvider`	✗ Non	✓ Oui	✗ Non
`AWS::ECS::Cluster`	✓ Oui	✓ Oui	✗ Non
`AWS::ECS::ContainerInstance`	✗ Non	✓ Oui	✗ Non
`AWS::ECS::Service`	✗ Non	✓ Oui	✗ Non
`AWS::ECS::Task`	✗ Non	✓ Oui	✗ Non
`AWS::ECS::TaskDefinition`	✓ Oui	✓ Oui	✗ Non
`AWS::ECS::TaskSet`	✗ Non	✓ Oui	✗ Non

Amazon Elastic File System

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EFS::FileSystem`	✓ Oui	✓ Oui	✓ Oui

Amazon Elastic Inference

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ElasticInference::ElasticInferenceAccelerator`	✓ Oui	✓ Oui	× Non

Amazon Elastic Kubernetes Service (Amazon EKS)

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EKS::Addon`	× Non	✓ Oui	× Non
`AWS::EKS::Cluster`	✓ Oui	✓ Oui	✓ Oui

Elastic Load Balancing

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ElasticLoadBalancing::LoadBalancer`	✓ Oui	✓ Oui	✓ Oui
`AWS::ElasticLoadBalancingV2::Listener`	× Non	✓ Oui	✓ Oui
`AWS::ElasticLoadBalancingV2::ListenerRule`	× Non	✓ Oui	✓ Oui
`AWS::ElasticLoadBalancingV2::LoadBalancer`	✓ Oui	✓ Oui	✓ Oui
`AWS::ElasticLoadBalancingV2::TargetGroup`	✓ Oui	✓ Oui	✓ Oui

Amazon OpenSearch Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Elasticsearch::Domain`	✓ Oui	✓ Oui	✓ Oui

CloudWatch Événements Amazon

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Events::EventBus`	✗ Non	✓ Oui	✗ Non
`AWS::Events::Rule`	✓ Oui	✓ Oui	✓ Oui

> **Note**
>
> Les règles des bus d'événements personnalisés ne sont pas prises en charge dans l'éditeur de balises.

EventBridge Schémas Amazon

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::EventSchemas::Discoverer`	✗ Non	✓ Oui	✗ Non
`AWS::EventSchemas::Registry`	✗ Non	✓ Oui	✗ Non
`AWS::EventSchemas::Schema`	✗ Non	✓ Oui	✗ Non

Amazon FSx

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::FSx::FileSystem`	✓ Oui	✓ Oui	× Non
`AWS::FSx::StorageVirtualMachine`	× Non	✓ Oui	× Non
`AWS::FSx::Volume`	× Non	✓ Oui	× Non

Amazon Forecast

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Forecast::Dataset`	✓ Oui	✓ Oui	× Non
`AWS::Forecast::DatasetGroup`	✓ Oui	✓ Oui	× Non
`AWS::Forecast::DatasetImportJob`	✓ Oui	✓ Oui	× Non
`AWS::Forecast::Forecast`	✓ Oui	✓ Oui	× Non
`AWS::Forecast::ForecastExportJob`	✓ Oui	✓ Oui	× Non
`AWS::Forecast::Predictor`	✓ Oui	✓ Oui	× Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Forecast::PredictorBacktestExportJob`	✓ Oui	✓ Oui	× Non

Amazon Fraud Detector

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::FraudDetector::Detector`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::DetectorVersion`	× Non	✓ Oui	× Non
`AWS::FraudDetector::EntityType`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::EventType`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::ExternalModel`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::Label`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::Model`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::ModelVersion`	× Non	✓ Oui	× Non
`AWS::FraudDetector::Outcome`	✓ Oui	✓ Oui	× Non
`AWS::FraudDetector::Rule`	× Non	✓ Oui	× Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::FraudDetector::Variable`	✓ Oui	✓ Oui	× Non

Amazon GameLift

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::GameLift::Alias`	× Non	✓ Oui	× Non
`AWS::GameLift::GameSessionQueue`	× Non	✓ Oui	× Non
`AWS::GameLift::Location`	× Non	✓ Oui	× Non
`AWS::GameLift::MatchmakingConfiguration`	× Non	✓ Oui	× Non
`AWS::GameLift::MatchmakingRuleSet`	× Non	✓ Oui	× Non

AWS Global Accelerator

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::GlobalAccelerator::Accelerator`	✗ Non	✓ Oui	✗ Non

AWS Glue

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Glue::Crawler`	✓ Oui	✓ Oui	✗ Non
`AWS::Glue::Database`	✗ Non	✓ Oui	✓ Oui
`AWS::Glue::Job`	✓ Oui	✓ Oui	✗ Non
`AWS::Glue::MLTransform`	✗ Non	✓ Oui	✗ Non
`AWS::Glue::Registry`	✗ Non	✓ Oui	✗ Non
`AWS::Glue::Trigger`	✓ Oui	✓ Oui	✗ Non
`AWS::Glue::Workflow`	✗ Non	✓ Oui	✗ Non

AWS Glue DataBrew

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::DataBrew::Dataset`	✓ Oui	✓ Oui	✓ Oui
`AWS::DataBrew::Job`	✓ Oui	✓ Oui	✓ Oui
`AWS::DataBrew::Project`	✓ Oui	✓ Oui	✓ Oui
`AWS::DataBrew::Recipe`	✓ Oui	✓ Oui	✓ Oui
`AWS::DataBrew::Schedule`	✓ Oui	✓ Oui	✓ Oui

AWS Ground Station

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::GroundStation::Config`	× Non	✓ Oui	× Non
`AWS::GroundStation::DataflowEndpointGroup`	× Non	✓ Oui	× Non
`AWS::GroundStation::MissionProfile`	× Non	✓ Oui	× Non

Amazon GuardDuty

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::GuardDuty::Detector`	✗ Non	✓ Oui	✓ Oui
`AWS::GuardDuty::Filter`	✗ Non	✓ Oui	✗ Non
`AWS::GuardDuty::IPSet`	✗ Non	✓ Oui	✗ Non
`AWS::GuardDuty::ThreatIntelSet`	✗ Non	✓ Oui	✗ Non

Amazon Interactive Video Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IVS::Channel`	✗ Non	✓ Oui	✗ Non
`AWS::IVS::RecordingConfiguration`	✗ Non	✓ Oui	✗ Non
`AWS::IVS::StreamKey`	✗ Non	✓ Oui	✗ Non

AWS Identity and Access Management

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IAM::InstanceProfile`	✓ Oui[1]	✓ Oui[2]	× Non
`AWS::IAM::ManagedPolicy`	✓ Oui[1]	✓ Oui[2]	× Non
`AWS::IAM::OpenIDConnectProvider`	✓ Oui[1]	✓ Oui[2]	× Non
`AWS::IAM::Role`	× Non	× Non	✓ Oui[2]
`AWS::IAM::SAMLProvider`	✓ Oui[1]	✓ Oui[2]	× Non
`AWS::IAM::ServerCertificate`	✓ Oui[1]	✓ Oui[2]	× Non
`AWS::IAM::VirtualMFADevice`	✓ Oui[1]	✓ Oui[2]	× Non

[1] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Pour utiliser l'éditeur de balises afin de créer ou de modifier des balises pour ce type `us-east-1` de ressource, vous devez les inclure dans la liste Sélectionner les régions sous Rechercher les ressources à étiqueter dans la console de l'éditeur de balises.

[2] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Les Resource Groups étant gérés séparément pour chaque région, vous devez passer AWS Management Console à celui Région AWS qui contient les ressources que vous souhaitez inclure dans le groupe. Pour créer un groupe de ressources contenant une ressource globale, vous devez configurer votre US-east-1 AWS Management Console à l'aide du sélecteur de région situé dans le coin supérieur droit du. AWS Management Console

EC2 Image Builder

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ImageBuilder::Component`	✗ Non	✓ Oui	✗ Non
`AWS::ImageBuilder::ContainerRecipe`	✗ Non	✓ Oui	✗ Non
`AWS::ImageBuilder::DistributionConfiguration`	✗ Non	✓ Oui	✗ Non
`AWS::ImageBuilder::Image`	✗ Non	✓ Oui	✗ Non
`AWS::ImageBuilder::ImagePipeline`	✗ Non	✓ Oui	✗ Non
`AWS::ImageBuilder::ImageRecipe`	✗ Non	✓ Oui	✗ Non
`AWS::ImageBuilder::InfrastructureConfiguration`	✗ Non	✓ Oui	✗ Non

Amazon Inspector

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Inspector::AssessmentTemplate`	✗ Non	✓ Oui	✓ Oui

AWS IoT

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoT::Authorizer`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::BillingGroup`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::CACertificate`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::CustomMetric`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::Dimension`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::JobTemplate`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::MitigationAction`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::Policy`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::RoleAlias`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::ScheduledAudit`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::SecurityProfile`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::ThingGroup`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::ThingType`	✗ Non	✓ Oui	✗ Non
`AWS::IoT::TopicRule`	✗ Non	✓ Oui	✓ Oui

AWS IoT Analytics

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoTAnalytics::Channel`	✗ Non	✓ Oui	✗ Non
`AWS::IoTAnalytics::Dataset`	✓ Oui	✓ Oui	✗ Non
`AWS::IoTAnalytics::Datastore`	✗ Non	✓ Oui	✗ Non
`AWS::IoTAnalytics::Pipeline`	✗ Non	✓ Oui	✗ Non

AWS IoT Events

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoTEvents::AlarmModel`	✗ Non	✓ Oui	✗ Non
`AWS::IoTEvents::DetectorModel`	✓ Oui	✓ Oui	✓ Oui
`AWS::IoTEvents::Input`	✓ Oui	✓ Oui	✓ Oui

AWS IoT FleetWise

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoTFleetWise::Campaign`	✗ Non	✓ Oui	✓ Oui
`AWS::IoTFleetWise::DecoderManifest`	✗ Non	✓ Oui	✓ Oui
`AWS::IoTFleetWise::Fleet`	✗ Non	✓ Oui	✓ Oui
`AWS::IoTFleetWise::ModelManifest`	✗ Non	✓ Oui	✓ Oui
`AWS::IoTFleetWise::SignalCatalog`	✗ Non	✓ Oui	✓ Oui
`AWS::IoTFleetWise::Vehicle`	✗ Non	✓ Oui	✓ Oui

AWS IoT Greengrass

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Greengrass::ConnectorDefinition`	✓ Oui	✓ Oui	✗ Non
`AWS::Greengrass::CoreDefinition`	✓ Oui	✓ Oui	✗ Non
`AWS::Greengrass::DeviceDefinition`	✓ Oui	✓ Oui	✗ Non
`AWS::Greengrass::FunctionDefinition`	✓ Oui	✓ Oui	✗ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Greengrass::Group`	✓ Oui	✓ Oui	× Non
`AWS::Greengrass::LoggerDefinition`	✓ Oui	✓ Oui	× Non
`AWS::Greengrass::ResourceDefinition`	✓ Oui	✓ Oui	× Non
`AWS::Greengrass::SubscriptionDefinition`	✓ Oui	✓ Oui	× Non

AWS IoT Greengrass Version 2

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::GreengrassV2::ComponentVersion`	× Non	✓ Oui	× Non

Console AWS IoT SiteWise

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoTSiteWise::Asset`	✗ Non	✓ Oui	✗ Non
`AWS::IoTSiteWise::AssetModel`	✗ Non	✓ Oui	✗ Non
`AWS::IoTSiteWise::Dashboard`	✗ Non	✓ Oui	✗ Non
`AWS::IoTSiteWise::Gateway`	✗ Non	✓ Oui	✗ Non
`AWS::IoTSiteWise::Portal`	✗ Non	✓ Oui	✗ Non
`AWS::IoTSiteWise::Project`	✗ Non	✓ Oui	✗ Non

AWS IoT Wireless

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoTWireless::Destination`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::DeviceProfile`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::FuotaTask`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::MulticastGroup`	✗ Non	✓ Oui	✗ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::IoTWireless::NetworkAnalyzerConfiguration`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::ServiceProfile`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::TaskDefinition`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::WirelessDevice`	✗ Non	✓ Oui	✗ Non
`AWS::IoTWireless::WirelessGateway`	✗ Non	✓ Oui	✗ Non

AWS Key Management Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::KMS::Alias`	✗ Non	✗ Non	✓ Oui
`AWS::KMS::Key`	✓ Oui	✓ Oui	✓ Oui

Amazon Keyspaces (pour Apache Cassandra)

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Cassandra::Keyspace`	✕ Non	✓ Oui	✓ Oui
`AWS::Cassandra::Table`	✕ Non	✓ Oui	✕ Non

Amazon Kinesis

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Kinesis::Stream`	✓ Oui	✓ Oui	✓ Oui

Service géré Amazon pour Apache Flink

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::KinesisAnalytics::Application`	✓ Oui	✓ Oui	✓ Oui

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::KinesisAnalyticsV2::Application`	✕ Non	✕ Non	✓ Oui

Amazon Data Firehose

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::KinesisFirehose::DeliveryStream`	✕ Non	✓ Oui	✓ Oui

AWS Lambda

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Lambda::Alias`	✕ Non	✕ Non	✓ Oui
`AWS::Lambda::EventSourceMapping`	✕ Non	✕ Non	✓ Oui
`AWS::Lambda::Function`	✓ Oui	✓ Oui	✓ Oui

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Lambda::LayerVersion`	✗ Non	✗ Non	✓ Oui
`AWS::Lambda::Version`	✗ Non	✗ Non	✓ Oui

Amazon Lightsail

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Lightsail::Bucket`	✗ Non	✓ Oui	✗ Non
`AWS::Lightsail::Certificate`	✗ Non	✓ Oui	✗ Non
`AWS::Lightsail::Container`	✗ Non	✓ Oui	✗ Non
`AWS::Lightsail::Disk`	✗ Non	✓ Oui	✗ Non
`AWS::Lightsail::Distribution`	✗ Non	✓ Oui	✗ Non
`AWS::Lightsail::Instance`	✗ Non	✓ Oui	✗ Non
`AWS::Lightsail::StaticIp`	✗ Non	✓ Oui	✗ Non

Amazon MQ

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::AmazonMQ::Broker`	✓ Oui	✓ Oui	× Non
`AWS::AmazonMQ::Configuration`	✓ Oui	✓ Oui	× Non

Amazon Macie

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Macie::ClassificationJob`	✓ Oui	✓ Oui	× Non
`AWS::Macie::CustomDataIdentifier`	✓ Oui	✓ Oui	✓ Oui
`AWS::Macie::FindingsFilter`	✓ Oui	✓ Oui	✓ Oui
`AWS::Macie::Member`	✓ Oui	✓ Oui	× Non

Amazon Managed Blockchain

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ManagedBlockchain::Accessor`	✗ Non	✓ Oui	✗ Non

Amazon Managed Streaming for Apache Kafka

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Kafka::Cluster`	✓ Oui	✓ Oui	✗ Non

AWS Elemental MediaConnect

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::MediaConnect::Flow`	✗ Non	✓ Oui	✗ Non
`AWS::MediaConnect::FlowEntitlement`	✗ Non	✓ Oui	✗ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::MediaConnect::FlowOutput`	✕ Non	✓ Oui	✕ Non
`AWS::MediaConnect::FlowSource`	✕ Non	✓ Oui	✕ Non

AWS Elemental MediaPackage

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::MediaPackage::Channel`	✕ Non	✓ Oui	✕ Non
`AWS::MediaPackage::PackagingConfiguration`	✕ Non	✓ Oui	✕ Non
`AWS::MediaPackage::PackagingGroup`	✕ Non	✓ Oui	✕ Non

AWS Network Manager

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::NetworkManager::CoreNetwork`	✕ Non	✓ Oui	✕ Non
`AWS::NetworkManager::Device`	✕ Non	✓ Oui	✕ Non
`AWS::NetworkManager::GlobalNetwork`	✕ Non	✓ Oui	✕ Non
`AWS::NetworkManager::Link`	✕ Non	✓ Oui	✕ Non
`AWS::NetworkManager::Site`	✕ Non	✓ Oui	✕ Non
`AWS::NetworkManager::VpcAttachment`	✕ Non	✓ Oui	✕ Non

Amazon OpenSearch Service OpenSearch

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::OpenSearchService::Domain`	✓ Oui	✓ Oui	✓ Oui

AWS OpsWorks

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::OpsWorks::Instance`	✗ Non	✓ Oui	✓ Oui
`AWS::OpsWorks::Layer`	✗ Non	✓ Oui	✓ Oui
`AWS::OpsWorks::Stack`	✗ Non	✓ Oui	✓ Oui

AWS Organizations

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Organizations::Account`	✓ Oui	✓ Oui	✗ Non
`AWS::Organizations::OrganizationalUnit`	✗ Non	✓ Oui	✗ Non
`AWS::Organizations::Policy`	✗ Non	✓ Oui	✗ Non
`AWS::Organizations::Root`	✓ Oui	✓ Oui	✗ Non

Amazon Pinpoint

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Pinpoint::App`	✕ Non	✓ Oui	✓ Oui
`AWS::Pinpoint::EmailTemplate`	✕ Non	✓ Oui	✓ Oui
`AWS::Pinpoint::PushTemplate`	✕ Non	✓ Oui	✓ Oui
`AWS::Pinpoint::SmsTemplate`	✕ Non	✓ Oui	✓ Oui
`AWS::Pinpoint::VoiceTemplate`	✕ Non	✓ Oui	✕ Non

API de messages SMS et vocaux Amazon Pinpoint

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::PinpointSMSVoiceV2::Pool`	✕ Non	✓ Oui	✕ Non

Amazon Quantum Ledger Database (Amazon QLDB)

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::QLDB::Ledger`	✓ Oui	✓ Oui	✓ Oui
`AWS::QLDB::Stream`	× Non	✓ Oui	✓ Oui

Amazon Redshift

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Redshift::Cluster`	✓ Oui	✓ Oui	✓ Oui
`AWS::Redshift::ClusterParameterGroup`	✓ Oui	✓ Oui	✓ Oui
`AWS::Redshift::ClusterSecurityGroup`	× Non	✓ Oui	✓ Oui
`AWS::Redshift::ClusterSubnetGroup`	✓ Oui	✓ Oui	✓ Oui
`AWS::Redshift::DBGroup`	× Non	✓ Oui	× Non
`AWS::Redshift::DBName`	× Non	✓ Oui	× Non
`AWS::Redshift::DBUser`	× Non	✓ Oui	× Non
`AWS::Redshift::EventSubscription`	× Non	✓ Oui	× Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Redshift::HSMClientCertificate`	✓ Oui	✓ Oui	× Non
`AWS::Redshift::HSMConfiguration`	× Non	✓ Oui	× Non
`AWS::Redshift::Namespace`	× Non	✓ Oui	× Non
`AWS::Redshift::Snapshot`	× Non	✓ Oui	× Non
`AWS::Redshift::SnapshotCopyGrant`	× Non	✓ Oui	× Non
`AWS::Redshift::SnapshotSchedule`	× Non	✓ Oui	× Non
`AWS::Redshift::UsageLimit`	× Non	✓ Oui	× Non

Amazon Relational Database Service (Amazon RDS)

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::RDS::CustomDBEngineVersion`	× Non	✓ Oui	× Non
`AWS::RDS::DBCluster`	✓ Oui	✓ Oui	✓ Oui
`AWS::RDS::DBClusterEndpoint`	× Non	✓ Oui	× Non
`AWS::RDS::DBClusterParameterGroup`	✓ Oui	✓ Oui	✓ Oui

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::RDS::DBClusterSnapshot`	✓ Oui	✓ Oui	× Non
`AWS::RDS::DBInstance`	✓ Oui	✓ Oui	✓ Oui
`AWS::RDS::DBParameterGroup`	✓ Oui	✓ Oui	✓ Oui
`AWS::RDS::DBProxy`	× Non	✓ Oui	× Non
`AWS::RDS::DBProxyEndpoint`	× Non	✓ Oui	× Non
`AWS::RDS::DBProxyTargetGroup`	× Non	✓ Oui	× Non
`AWS::RDS::DBSecurityGroup`	✓ Oui	✓ Oui	✓ Oui
`AWS::RDS::DBSnapshot`	✓ Oui	✓ Oui	× Non
`AWS::RDS::DBSubnetGroup`	✓ Oui	✓ Oui	✓ Oui
`AWS::RDS::Deployment`	× Non	✓ Oui	× Non
`AWS::RDS::EventSubscription`	✓ Oui	✓ Oui	× Non
`AWS::RDS::OptionGroup`	✓ Oui	✓ Oui	× Non
`AWS::RDS::ReservedDBInstance`	✓ Oui	✓ Oui	× Non

AWS Resource Access Manager

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::RAM::ResourceShare`	✓ Oui	✓ Oui	× Non

AWS Resource Groups

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ResourceGroups::Group`	✓ Oui	✓ Oui	✓ Oui

AWS Robomaker

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::RoboMaker::DeploymentJob`	× Non	✓ Oui	× Non
`AWS::RoboMaker::Fleet`	× Non	✓ Oui	× Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::RoboMaker::Robot`	✗ Non	✓ Oui	✗ Non
`AWS::RoboMaker::RobotApplication`	✓ Oui	✓ Oui	✗ Non
`AWS::RoboMaker::SimulationApplication`	✓ Oui	✓ Oui	✗ Non
`AWS::RoboMaker::SimulationJob`	✓ Oui	✓ Oui	✗ Non

Amazon Route 53

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Route53::Domain`	✓ Oui[1]	✓ Oui[2]	✗ Non
`AWS::Route53::HealthCheck`	✓ Oui[1]	✓ Oui[2]	✓ Oui[2]
`AWS::Route53::HostedZone`	✓ Oui[1]	✓ Oui[2]	✓ Oui[2]

[1] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Pour utiliser l'éditeur de balises afin de créer ou de modifier des balises pour ce type `us-east-1` de ressource, vous devez les inclure dans la liste Sélectionner les régions sous Rechercher les ressources à étiqueter dans la console de l'éditeur de balises.

[2] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Les Resource Groups étant gérés séparément pour chaque région, vous devez passer AWS Management Console à celui Région AWS qui contient les ressources que vous souhaitez inclure dans le groupe. Pour créer un groupe de ressources contenant une ressource globale, vous devez configurer votre US-east-1 AWS Management Console à l'aide du sélecteur de région situé dans le coin supérieur droit du. AWS Management Console

Amazon Route 53 Resolver

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Route53Resolver::FirewallDomainList`	✕ Non	✓ Oui[2]	✕ Non
`AWS::Route53Resolver::FirewallRuleGroup`	✕ Non	✓ Oui[2]	✕ Non
`AWS::Route53Resolver::FirewallRuleGroupAssociation`	✕ Non	✓ Oui[2]	✕ Non
`AWS::Route53Resolver::ResolverEndpoint`	✓ Oui[1]	✓ Oui[2]	✕ Non
`AWS::Route53Resolver::ResolverQueryLoggingConfig`	✕ Non	✓ Oui[2]	✕ Non
`AWS::Route53Resolver::ResolverRule`	✓ Oui[1]	✓ Oui[2]	✕ Non

[1] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Pour utiliser l'éditeur de balises afin de créer ou de modifier des balises pour ce type `us-east-1` de ressource, vous devez les inclure dans la liste Sélectionner les régions sous Rechercher les ressources à étiqueter dans la console de l'éditeur de balises.

[2] Il s'agit d'une ressource pour un service mondial hébergé dans la région USA Est (Virginie du Nord). Les Resource Groups étant gérés séparément pour chaque région, vous devez passer AWS Management Console à celui Région AWS qui contient les ressources que vous souhaitez inclure dans le groupe. Pour créer un groupe de ressources contenant une ressource globale, vous devez configurer votre US-east-1 AWS Management Console à l'aide du sélecteur de région situé dans le coin supérieur droit du. AWS Management Console

Amazon S3 Glacier

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Glacier::Vault`	✓ Oui	✓ Oui	× Non

Amazon SageMaker

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SageMaker::AppImageConfig`	× Non	✓ Oui	× Non
`AWS::SageMaker::CodeRepository`	× Non	✓ Oui	× Non
`AWS::SageMaker::Endpoint`	× Non	✓ Oui	✓ Oui
`AWS::SageMaker::EndpointConfig`	× Non	✓ Oui	✓ Oui

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SageMaker::HyperParameterTuningJob`	✗ Non	✓ Oui	✗ Non
`AWS::SageMaker::Image`	✗ Non	✓ Oui	✗ Non
`AWS::SageMaker::LabelingJob`	✗ Non	✓ Oui	✗ Non
`AWS::SageMaker::Model`	✗ Non	✓ Oui	✓ Oui
`AWS::SageMaker::ModelPackageGroup`	✗ Non	✓ Oui	✓ Oui
`AWS::SageMaker::NotebookInstance`	✓ Oui	✓ Oui	✓ Oui
`AWS::SageMaker::Pipeline`	✗ Non	✓ Oui	✗ Non
`AWS::SageMaker::Project`	✗ Non	✓ Oui	✓ Oui
`AWS::SageMaker::TrainingJob`	✗ Non	✓ Oui	✗ Non
`AWS::SageMaker::TransformJob`	✗ Non	✓ Oui	✗ Non
`AWS::SageMaker::Workteam`	✗ Non	✓ Oui	✗ Non

AWS Secrets Manager

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SecretsManager::Secret`	✓ Oui	✓ Oui	✓ Oui

AWS Service Catalog

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ServiceCatalog::CloudFormationProduct`	× Non	✓ Oui	✓ Oui
`AWS::ServiceCatalog::Portfolio`	× Non	✓ Oui	✓ Oui

AWS Service Catalog AppRegistry

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ServiceCatalogAppRegistry::Application`	✕ Non	✓ Oui	✕ Non
`AWS::ServiceCatalogAppRegistry::AttributeGroup`	✕ Non	✓ Oui	✕ Non

Service Quotas

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::ServiceQuotas::Quota`	✕ Non	✓ Oui	✕ Non

Amazon Simple Email Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SES::ConfigurationSet`	✓ Oui	✓ Oui	✓ Oui
`AWS::SES::ContactList`	✓ Oui	✓ Oui	✓ Oui
`AWS::SES::DedicatedIpPool`	✓ Oui	✓ Oui	× Non
`AWS::SES::Identity`	✓ Oui	✓ Oui	× Non

Amazon Simple Notification Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SNS::Topic`	✓ Oui	✓ Oui	✓ Oui

Amazon Simple Queue Service

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SQS::Queue`	✓ Oui	✓ Oui	✓ Oui

Amazon Simple Storage Service (Amazon S3)

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::S3::Bucket`	✓ Oui	✓ Oui	✓ Oui
`AWS::S3::Job`	× Non	✓ Oui	× Non
`AWS::S3::StorageLens`	× Non	✓ Oui	× Non

AWS Step Functions

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::StepFunctions::Activity`	✓ Oui	✓ Oui	✓ Oui
`AWS::StepFunctions::StateMachine`	✓ Oui	✓ Oui	✓ Oui

Storage Gateway

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::StorageGateway::Gateway`	✓ Oui	✓ Oui	× Non
`AWS::StorageGateway::Volume`	× Non	✓ Oui	× Non

AWS Systems Manager

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SSM::Association`	✗ Non	✓ Oui	✗ Non
`AWS::SSM::AutomationExecution`	✗ Non	✓ Oui	✗ Non
`AWS::SSM::Document`	✗ Non	✓ Oui	✓ Oui
`AWS::SSM::MaintenanceWindow`	✗ Non	✓ Oui	✗ Non
`AWS::SSM::ManagedInstance`	✗ Non	✓ Oui	✗ Non
`AWS::SSM::OpsItem`	✗ Non	✓ Oui	✗ Non
`AWS::SSM::OpsMetadata`	✗ Non	✓ Oui	✗ Non
`AWS::SSM::Parameter`	✓ Oui	✓ Oui	✓ Oui
`AWS::SSM::PatchBaseline`	✗ Non	✓ Oui	✓ Oui

AWS Systems Manager pour SAP

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SystemsManagerSAP::Application`	✗ Non	✓ Oui	✓ Oui

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::SystemsManagerSAP::Database`	✕ Non	✓ Oui	✕ Non

Amazon Timestream

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Timestream::ScheduledQuery`	✕ Non	✓ Oui	✓ Oui

AWS Transfer Family

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Transfer::Certificate`	✕ Non	✓ Oui	✕ Non
`AWS::Transfer::Connector`	✕ Non	✓ Oui	✕ Non
`AWS::Transfer::Profile`	✕ Non	✓ Oui	✕ Non

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::Transfer::Workflow`	✕ Non	✓ Oui	✕ Non

AWS WAF

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::WAF::Rule`	✕ Non	✓ Oui	✕ Non
`AWS::WAF::WebACL`	✕ Non	✓ Oui	✕ Non

Amazon WorkSpaces

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::WorkSpaces::Workspace`	✓ Oui	✓ Oui	✓ Oui

AWS X-Ray

Ressources	Balisage de l'éditeur de balises	Groupes basés sur des balises	AWS CloudFormation Groupes basés sur des piles
`AWS::XRay::Group`	✗ Non	✓ Oui	✗ Non
`AWS::XRay::SamplingRule`	✗ Non	✓ Oui	✗ Non

Types de ressources déconseillés

Les types de ressources suivants ne sont plus pris en charge pour les fonctionnalités spécifiées.

Service	Type de ressource	Support au changement	Date
AWS RoboMaker	`AWS::RoboMaker::Robot`	N'est plus pris en charge par Tag Editor.	2 mai 2022
AWS RoboMaker	`AWS::RoboMaker::Fleet`	N'est plus pris en charge par Tag Editor.	2 mai 2022
AWS RoboMaker	`AWS::RoboMaker::DeploymentJob`	N'est plus pris en charge par Tag Editor.	2 mai 2022

Création de groupes de ressources avec AWS CloudFormation

AWS Resource Groups est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (telles que les groupes de ressources), et qui AWS CloudFormation fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos groupes de ressources de manière cohérente et répétée. Décrivez vos groupes de ressources une seule fois, puis provisionnez les mêmes groupes de ressources à plusieurs reprises dans plusieurs Comptes AWS régions.

Resource Groups et AWS CloudFormation modèles

Pour fournir et configurer des ressources pour Resource Groups et les services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés dans JSON ouYAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous ne connaissez pas JSON ouYAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, voir Qu'est-ce que AWS CloudFormation Designer ? dans le guide de AWS CloudFormation l'utilisateur.

Resource Groups permet de créer des groupes de ressources dans AWS CloudFormation. Pour plus d'informations, notamment des exemples JSON et des YAML modèles de groupes de ressources, consultez la référence au type de AWS Resource Groups ressource dans le guide de AWS CloudFormation l'utilisateur.

En savoir plus sur AWS CloudFormation

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

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation APIRéférence

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

Sécurité dans AWS Resource Groups

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

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

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

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Resource Groups. Les rubriques suivantes vous montrent comment configurer les Resource Groups pour qu'ils répondent à vos objectifs de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autresAWSles services qui vous aident à surveiller et sécuriser vos ressources de Resource Groups.

Rubriques

- Protection des données dans AWS Resource Groups
- Gestion des identités et des accès pour AWS Resource Groups
- Journalisation et surveillance dans les Resource Groups
- Validation de conformité pour Resource Groups
- Résilience dans les Resource Groups
- Sécurité de l'infrastructure dans Resource Groups
- Éonnes pour les groupes de sécurité pour les Resource Groups sécurité pour

Protection des données dans AWS Resource Groups

Le AWS modèle de responsabilité partagée modèle s'applique à la protection des données dans AWS Resource Groups. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. Vous êtes responsable du contrôle de votre contenu hébergé sur cette infrastructure. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour 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 AWS Modèle de responsabilité partagée et article de GDPR blog sur le AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS IAM Identity Center or 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 AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation CloudTrail des sentiers pour capturer AWS activités, voir Travailler avec les CloudTrail sentiers dans le AWS CloudTrail Guide de l'utilisateur.
- Utiliser AWS solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut intégrés 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 FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Resource Groups 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 y inclure d'informations d'identification URL pour valider votre demande auprès de ce serveur.

Chiffrement des données

Comparé à d'autres AWS des services, AWS Resource Groups possède une surface d'attaque minimale, car il ne permet pas de modifier, d'ajouter ou de supprimer AWS ressources sauf pour les groupes. Resource Groups collecte auprès de vous les informations spécifiques aux services suivantes.

- Noms de groupe (non chiffrés, non privés)
- Descriptions de groupe (non cryptées, mais privées)
- Ressources des membres dans des groupes (elles sont stockées dans des journaux, qui ne sont pas cryptés)

Chiffrement au repos

Il n'existe aucun autre moyen d'isoler le trafic de service ou réseau spécifique à Resource Groups. Le cas échéant, utilisez AWS-isolation spécifique. Vous pouvez utiliser les Resource Groups API et la console VPC pour optimiser la confidentialité et la sécurité de l'infrastructure.

Chiffrement en transit

AWS Resource Groups les données sont cryptées lors de leur transfert vers la base de données interne du service à des fins de sauvegarde. Ceci n'est pas configurable par l'utilisateur.

Gestion des clés

AWS Resource Groups n'est actuellement pas intégré à AWS Key Management Service et ne prend pas en charge AWS KMS keys.

Confidentialité du trafic inter-réseau

AWS Resource Groups utilise HTTPS pour toutes les transmissions entre les utilisateurs de Resource Groups et AWS. Resource Groups utilise transport layer security (TLS) 1.2, mais prend également en charge les TLS versions 1.0 et 1.1.

Gestion des identités et des accès pour AWS Resource Groups

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

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment Resource Groups travaille avec IAM
- Politiques AWS gérées pour AWS Resource Groups
- Utilisation des rôles liés à un service pour les Resource Groups pour les groupes de ressources
- Exemples de politiques basées sur l'identité AWS Resource Groups
- Résolution des problèmes AWS Resource Groups d'identité et d'accès

Public ciblé

Comment utilisez-vous AWS Identity and Access Management (IAM) diffère en fonction du travail que vous effectuez dans Resource Groups.

Utilisateur du service : si vous utilisez le service Resource Groups 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 Resource Groups pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Resource Groups, consultezRésolution des problèmes AWS Resource Groups d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des ressources Resource Groups dans votre entreprise, vous avez probablement un accès complet à Resource Groups. C'est à vous de déterminer les fonctionnalités et les ressources de Resource Groups auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette

page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM Resource Groups, consultezComment Resource Groups travaille 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 aux Resource Groups. Pour consulter des exemples de politiques basées sur l'identité de Resource Groups que vous pouvez utiliserIAM, consultez. Exemples de politiques basées sur l'identité AWS Resource Groups

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS en utilisant 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 à AWS en 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 AWS en utilisant la fédération, vous assumez indirectement un rôle.

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

Si vous accédez AWS programmatiquement, 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 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, voir Signature AWS APIdemandes 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, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez la section Authentification multifactorielle dans le AWS IAM Identity Center Guide de l'utilisateur et utilisation de l'authentification multifactorielle (MFA) dans AWS dans le guide de l'utilisateur IAM.

Compte AWS utilisateur root

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

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de votre Compte AWS qui dispose d'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.

IAMrôles

Un IAMrôle est une identité au sein de votre Compte AWS qui dispose 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 AWS Management Console en changeant de rôle. Vous pouvez assumer un rôle en appelant un AWS CLI or AWS APIopération ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles 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 ensembles d'autorisations, voir Ensembles d'autorisations dans le AWS IAM Identity Center Guide de l'utilisateur.
- 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. Cependant, avec certains Services AWS, 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 utiliser 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 dans AWS, vous êtes considéré comme un directeur. 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 un Service AWS, combiné 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 nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives à l'envoi de FAS 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, voir Création d'un rôle pour déléguer des autorisations à un Service AWS dans le guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle lié à un service Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS 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 créent AWS CLI or AWS APIdemandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS pour attribuer un rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous créez 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 dans AWS en créant des politiques et en les associant à AWS identités ou ressources. Une politique est un objet dans AWS qui, lorsqu'elle est associée 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 dans 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 JSONpolitiques 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, le AWS CLI, ou le 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 dans votre Compte AWS. Les politiques gérées incluent AWS politiques gérées et 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 AWS politiques gérées à partir IAM d'une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

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

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

Autres types de politique

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

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

les comptes des membres, y compris chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et SCPs consultez les politiques de contrôle des services dans le AWS Organizations Guide de 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 détermine s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, voir la logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment Resource Groups travaille avec IAM

Avant de gérer l'IAMaccès à Resource Groups, vous devez connaître les IAM fonctionnalités disponibles avec Resource Groups. Pour obtenir une vue d'ensemble du fonctionnement des Resource Groups et AWS des autres servicesIAM, consultez la section AWS Services That Work with IAM du guide de IAM l'utilisateur.

Rubriques

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

Politiques basées sur l'identité de Resource Groups

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Resource Groups 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 section Référence des éléments de IAM JSON stratégie dans le guide de IAM l'utilisateur.

Actions

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

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

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

Les actions politiques dans Resource Groups utilisent le préfixe suivant avant l'action :`resource-groups:`. Les actions de l'éditeur de balises sont entièrement exécutées dans la console, mais le préfixe figure `resource-explorer` dans les entrées du journal.

Par exemple, pour autoriser quelqu'un à créer un groupe Resource Groups avec l'`CreateGroup`APIopération Resource Groups, vous devez inclure l'`resource-groups:CreateGroup`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Resource Groups définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions Resource Groups et Tag Editor dans une seule instruction, séparez-les par des virgules comme suit :

```
"Action": [
      "resource-groups:action1",
      "resource-groups:action2",
      "resource-explorer:action3"
```

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

```
"Action": "resource-groups:List*"
```

Pour consulter la liste des actions de Resource Groups, reportez-vous à la section Actions, Resources et Condition Keys du guide de IAM l'utilisateur. AWS Resource Groups

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": "*"
```

La seule ressource Resource Groups est un groupe. La ressource du groupe a ARN le format suivant :

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

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

Par exemple, pour spécifier le groupe de `my-test-group` ressources dans votre relevé, utilisez ce qui suit ARN :

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

Pour spécifier tous les groupes appartenant à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

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

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

Certaines API actions de Resource Groups peuvent impliquer plusieurs ressources. `DeleteGroup`Supprime par exemple des groupes, de sorte que le principal appelant doit être autorisé à supprimer un groupe spécifique ou tous les groupes. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules.

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

Pour consulter la liste des types de ressources Resource Groups et leurs caractéristiquesARNs, et pour savoir avec quelles actions vous pouvez spécifier les ARN ressources associées à chaque ressource, reportez-vous à la section Actions, Resources, and Condition Keys du guide de l'IAMutilisateur. AWS Resource Groups

Clés de condition

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.

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

Pour consulter la liste des clés de condition de Resource Groups et savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions, Resources et Condition Keys du guide de l'IAMutilisateur. AWS Resource Groups

Exemples

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

Politiques basées sur les ressources

Resource Groups ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises Resource Groups

Vous pouvez associer des balises à des groupes dans Resource Groups ou transmettre des balises dans une demande à Resource Groups. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Vous pouvez appliquer des balises à un groupe lorsque vous créez ou mettez à jour le groupe. Pour plus d'informations sur le balisage d'un groupe dans Resource Groups, consultez Création de groupes basés sur des requêtes dans AWS Resource Groups et Mettre à jour des groupes dans AWS Resource Groups dans ce guide.

Pour visualiser un exemple de politique basée sur l'identité permettant de limiter l'accès à une ressource en fonction des balises de cette ressource, consultez Affichage des groupes en fonction des balises.

IAMRôles de Resource Groups

Un IAMrôle est une entité de votre AWS compte qui possède des autorisations spécifiques. Resource Groups ne possède ni n'utilise de rôles de service.

Utilisation d'informations d'identification temporaires avec Resource Groups

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

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom.

Resource Groups ne possède ni n'utilise de rôles liés à un service.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom.

Resource Groups ne possède ni n'utilise de rôles de service.

Politiques AWS gérées pour AWS Resource Groups

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

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

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est

plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

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

AWS-politiques gérées pour les groupes de ressources

- ResourceGroupsServiceRolePolicy

AWS Politique gérée par: ResourceGroupsServiceRolePolicy

Vous ne pouvez pas joindre`ResourceGroupsServiceRolePolicy`à toutes les entités IAM vous-même. Cette politique ne peut être associée qu'à un rôle lié à un service qui permet aux groupes de ressources d'effectuer des actions en votre nom. Pour plus d'informations, veuillez consulter Utilisation des rôles liés à un service pour les Resource Groups pour les groupes de ressources.

Cette politique accorde les autorisations requises aux groupes de ressources pour récupérer des informations sur les ressources de vos groupes de ressources et sur toutesAWS CloudFormationles piles auxquelles ces ressources appartiennent. Cela permet aux groupes de ressources de générerCloudWatchÉvénements pour la fonctionnalité d'événements du cycle de vie du groupe.

Pour voir la dernière version de ceAWSpolitique gérée, voir`ResourceGroupsServiceRolePolicy`dans la console IAM.

AWSpolitique gérée : ResourceGroupsandTagEditorFullAccess

Lorsque vous attachez une politique à une entité principale, vous accordez à l'entité les autorisations définies dans la politique.AWSles politiques gérées vous permettent d'attribuer plus facilement les autorisations appropriées aux utilisateurs, aux groupes et aux rôles que si vous deviez les rédiger vous-même.

Cette politique accorde les autorisations requises pour un accès complet aux fonctionnalités des groupes de ressources et de l'éditeur de balises.

Pour voir la dernière version de ceAWSpolitique gérée, voir`ResourceGroupsandTagEditorFullAccess`dans la console IAM.

Pour plus d'informations sur cette politique, voir ResourceGroupsandTagEditorFullAccessdans leAWSGuide de référence des politiques gérées.

AWSpolitique gérée : ResourceGroupsandTagEditorReadOnlyAccès

Lorsque vous attachez une politique à une entité principale, vous accordez à l'entité les autorisations définies dans la politique.AWSles politiques gérées vous permettent d'attribuer plus facilement les autorisations appropriées aux utilisateurs, aux groupes et aux rôles que si vous deviez les rédiger vous-même.

Cette politique accorde les autorisations requises pour l'accès en lecture seule aux fonctionnalités des groupes de ressources et de l'éditeur de balises.

Pour voir la dernière version de ceAWSpolitique gérée, voir`ResourceGroupsandTagEditorReadOnlyAccess`dans la console IAM.

Pour plus d'informations sur cette politique, voir ResourceGroupsandTagEditorReadOnlyAccèsdans leAWSGuide de référence des politiques gérées.

Mises à jour des groupes de ressources versAWSpolitiques gérées

Afficher les détails des mises à jour deAWSpolitiques gérées pour les groupes de ressources depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS duGroupes de ressources Historique des documentspage.

Modification	Description	Date
Mise à jour de la politique —ResourceGroupsandTagEditorFullAccess	Les groupes de ressources ont mis à jour une politique pour inclure d'autresAWS CloudFormationautorisations.	10 août 2023
Mise à jour de la politique —ResourceGroupsandTagEditorReadOnlyAccess	Les groupes de ressources ont mis à jour une politique pour inclure d'autresAWS CloudFormationautorisations.	10 août 2023
Nouvelle politique —ResourceGroupsServiceRolePolicy	Resource Groups a ajouté une nouvelle politique pour soutenir son rôle lié aux services.	17 novembre 2022

Modification	Description	Date
Les groupes de ressources ont commencé à suivre les modifications	Resource Groups a commencé à suivre les modifications apportées à sonAWSpolitiques gérées.	17 novembre 2022

Utilisation des rôles liés à un service pour les Resource Groups pour les groupes de ressources

AWS Resource Groups utilise des rôles AWS Identity and Access Management (IAM) liés aux services. Un rôle lié à un service est un type unique de rôle IAM lié directement à des Resource Groups. Les rôles liés à un service sont prédéfinis par les Resource Groups et comprennent toutes les autorisations nécessaires au service pour appeler d'autresServices AWS personnes en votre nom.

Un rôle lié à un service simplifie la configuration des Resource Groups, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Les autorisations de ses rôles liés à un service et définit des politiques de confiance pour chacun de ses rôles liés à un service et, pour chacun d'entre eux, seul la fonction de ses rôles liés à un service et définit des politiques de confiance pour chacun de ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

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

Autorisations de rôles liés à un service pour les Resource Groups

Resource Groups rôles liés à un service suivant pour prendre en charge les événements du cycle de vie du groupe pour prendre en charge les événements du cycle de vie des groupes Cliquez sur le lien sur le nom du rôle pour afficher le rôle dans la console IAM après l'avoir créé.

- `AWSServiceRoleForResourceGroups`

Les Resource Groups utilisent les autorisations de ce rôle pour interroger lesServices AWS propriétaires de vos ressources afin de résoudre le problème de l'appartenance au groupe et de conserver le groupe up-to-date. Il permet aux Resource Groups d'envoyer des événements liés au EventBridge service Amazon.

Le rôle`AWSServiceRoleForResourceGroups` lié à un service approuve le service suivant pour assumer le rôle :

- `resourcegroups.amazonaws.com`

Les autorisations associées au rôle proviennent de la politiqueAWS gérée suivante. Cliquez sur le lien du nom de la politique pour afficher la politique dans la console IAM.

- `Politiques AWS gérées pour AWS Resource Groups`

Création du rôle lié à un service pour les Resource Groups pour les groupes de ressources

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous effectuez dans un autre service une action qui nécessite les fonctions prises en charge par ce rôle. Pour plus d'informations, consultez Un nouveau rôle est apparu dans monCompte AWS.

Pour créer le rôle lié à un service, activez la fonction d'événements du cycle de vie de groupe.

Modification d'un rôle lié à un service pour les Resource Groups pour les groupes de ressources

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

Suppression d'un rôle lié à un service pour les Resource Groups

Vous pouvez supprimer le rôle lié à un service après que vous avez désactivé la fonction d'événements du cycle de vie de groupe.

> **Important**
>
> - AWSvous empêche de supprimer le rôle lié au service tant que vous n'avez pas désactivé pour la première fois la fonctionnalité d'événements du cycle de vie des groupes qui l'a créé.
> - Nous vous recommandons de ne pas supprimer le rôle lié au service tant que votre rôle comporte des groupes de ressourcesCompte AWS. Le service Resource Groups ne peut pas interagir avec d'autres personnesServices AWS pour gérer vos groupes si vous supprimez ce rôle.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, AWS CLI, ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForResourceGroups. Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Console

Pour supprimer le rôle lié à un service Resource Groups de service

1. Ouvrez la console IAM sur la page Rôles.
2. Recherchez le rôle nommé AWSServiceRoleForResourceGroups et cochez la case à côté de celui-ci.
3. Sélectionnez Delete (Supprimer).
4. Confirmez votre intention de supprimer le rôle en saisissant le nom du rôle dans la zone, puis en choisissant Supprimer.

Le rôle disparaît de votre liste de rôles dans la console IAM.

AWS CLI

Pour supprimer le rôle lié à un service Resource Groups de service

Pour supprimer le rôle, saisissez la commande suivante avec les paramètres exactement comme indiqué. Ne remplacez aucune des valeurs.

```
$ aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForResourceGroups
{
    "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
}
```

La commande renvoie un ID de tâche. La suppression effective du rôle se produit de manière asynchrone. Vous pouvez vérifier l'état de la suppression du rôle en transmettant l'identificateur de tâche fourni à laAWS CLI commande suivante.

```
$ aws iam get-service-linked-role-deletion-status \
    --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
{
    "Status": "SUCCEEDED"
}
```

Régions prises en charge pour les rôles liés à un service des Resource Groups

Resource Groups de capacité prennent en charge l'utilisation des rôles liés à un service dans tous les domainesRégions AWS où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS.

Exemples de politiques basées sur l'identité AWS Resource Groups

Par défaut, les principaux IAM, tels que les rôles et les utilisateurs, ne sont pas autorisés à créer ou modifier les ressources des Resource Groups. Ils ne peuvent pas non plus exécuter des tâches à l'aide de la AWS Management Console, l'AWS CLI ou de l'API AWS. Un administrateur IAM doit créer des stratégies IAM autorisant les responsables à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux principaux qui ont besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console et de l'API Resource Groups
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Affichage des groupes en fonction des balises

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer Resource Groups de 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, veuillez consulter 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, veuillez consulter 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 compteCompte AWS, activez une MFA pour plus de sécurité. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, veuillez consulter 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, veuillez consulter Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console et de l'API Resource Groups

Pour accéder à la consoleAWS Resource Groups et à l'API de l'éditeur de balises, vous devez disposer d'un jeu minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources des Resource Groups de votreAWS compte. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console et les commandes d'API ne fonctionneront pas comme prévu pour les principaux utilisateurs (rôles IAM et utilisateurs) tributaires de cette stratégie.

Pour garantir que ces entités pourront continuer d'utiliser les Resource Groups, attachez la stratégie suivante (ou une stratégie qui contient les autorisations répertoriées dans la stratégie suivante) aux entités. Pour en savoir plus, consultez Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
```

```
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour de plus amples informations sur l'ensemble d'autorisations d'accès aux Resource Groups,Octroi d'autorisations d'utilisation AWS Resource Groups et éditeur de balises veuillez consulter dans ce guide.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations 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": "*"
        }
    ]
}
```

Affichage des groupes en fonction des balises

Vous pouvez utiliser des conditions dans votre stratégie basée sur l'identité pour contrôler l'accès aux ressources des Resource Groups en fonction des balises. Cet exemple montre comment créer une stratégie qui permet d'afficher une ressource, dans cet exemple, un groupe de ressources. Toutefois, l'autorisation est accordée uniquement si l'étiquette de groupe`project` a la même valeur que l'`project`étiquette attachée au principal appelant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

Vous pouvez attacher cette stratégie aux principaux de votre compte. Si un responsable possédant la clé de balise`project` et la valeur de balise`alpha` tente de visualiser un groupe de ressources,

le groupe doit également être balisé`project=alpha`. Dans le cas contraire, l'accès est refusé à l'utilisateur. La clé de condition d'étiquette `project` correspond à la fois à `Project` et à `project`, 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.

Résolution des problèmes AWS Resource Groups d'identité et d'accès

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Resource Groups et IAM.

Rubriques

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

Je ne suis pas autorisé à effectuer une action dans Resource Groups

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` essaie d'utiliser la console pour afficher les détails d'un groupe sans y être `resource-groups:ListGroups` autorisé.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: resource-groups:ListGroups on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `my-test-group` à l'aide de l'action `resource-groups:ListGroups`.

Je ne suis pas autorisé à effectuer iam : PassRole

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

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

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

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

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

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

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes Resource Groups

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 Groups prend en charge ces fonctionnalités, consultezComment Resource Groups travaille 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 connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Journalisation et surveillance dans les Resource Groups

Toutes lesAWS Resource Groups actions sont enregistréesAWS CloudTrail.

Journalisation des appels d'API AWS Resource Groups avec AWS CloudTrail

AWS Resource Groupset l'éditeur des actions effectuées par un utilisateurAWS CloudTrail, un rôle, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWS service dans des Resource Groups ou l'éditeur des événements. CloudTrail capture tous les appels d'API pour les Resource Groups en tant qu'événements, y compris les appels depuis la console Resource Groups appels depuis la console des appels des appels des appels des appels des appels des appels des appels des appels des appels des API des appels Resource Groups appels des appels des appels des appels des appels des appels des appels des Si vous créez un journal de suivi, vous pouvez activer la livraison continue des CloudTrail événements dans un compartiment Amazon S3, y compris des événements pour des Resource Groups. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Event history (Historique des événements). À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée aux Resource Groups, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres informations.

Pour en savoir plus CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

Informations sur les Resource Groups dans CloudTrail

CloudTrail est activé dans votreAWS compte lors de la création de ce dernier. Quand une activité se produit dans des Resource Groups ou dans la console des événements, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements deAWS service dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les

événements récents dans votre AWS compte. Pour de plus amples informations, veuillez consulter des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votreAWS compte, y compris les événements pour les Resource Groups, créez un journal d'activité. Un journal CloudTrail de suivi permet des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions. Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour plus d'informations, veuillez consulter les rubriques :

- Présentation de la création d'un journal d'activité
- Intégrations et services supportés par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception des fichiers CloudTrail journaux de plusieurs régions et Réception des fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions des Resource Groups sont consignées CloudTrail et documentées dans la Référence desAWS Resource Groups API. Les actions des Resource Groups CloudTrail sont affichées sous forme d'événements dont le point de terminaison`resource-groups.amazonaws.com` de l'API est la source. Par exemple, les appels au`UpdateGroupQuery` actions`CreateGroup``GetGroup`, et génèrent des entrées dans les fichiers CloudTrail journaux. Les actions de l'éditeur de balises dans la console sont enregistrées et sont affichées sous forme d'événements dont le point de terminaison`resource-explorer` interne de l'API est la source. CloudTrail

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les autorisations utilisateur racine ou IAM.
- Si la demande a été effectuée avec des autorisations de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez l'élément `userIdentity` CloudTrail.

Resource Groups fichiers journaux

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. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs des des des fichiers journaux. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. CloudTrail Les fichiers journaux ne constituent pas une trace de pile ordonnée des appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'action`CreateGroup`.

```
{"eventVersion":"1.05",
"userIdentity":{
    "type":"AssumedRole",
    "principalId":"ID number:AWSResourceGroupsUser",
    "arn":"arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
    "accountId":"831000000000","accessKeyId":"ID number",
    "sessionContext":{
        "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2018-06-05T22:03:47Z"
            },
        "sessionIssuer":{
            "type":"Role",
            "principalId":"ID number",
            "arn":"arn:aws:iam::831000000000:role/Admin",
            "accountId":"831000000000",
            "userName":"Admin"
            }
        }
    },
"eventTime":"2018-06-05T22:18:23Z",
"eventSource":"resource-groups.amazonaws.com",
"eventName":"CreateGroup",
"awsRegion":"us-west-2",
"sourceIPAddress":"100.25.190.51",
"userAgent":"console.amazonaws.com",
"requestParameters":{
    "Description": "EC2 instances that we are using for application staging.",
    "Name": "Staging",
    "ResourceQuery": {
```

```
      "Query": "string",
      "Type": "TAG_FILTERS_1_0"
      },
    "Tags": {
      "Key":"Phase",
      "Value":"Stage"
      }
    },
"responseElements":{
    "Group": {
      "Description":"EC2 instances that we are using for application staging.",
      "groupArn":"arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
      "Name":"Staging"
     },
    "resourceQuery": {
      "Query":"string",
      "Type":"TAG_FILTERS_1_0"
     }
    },
"requestID":"de7z64z9-d394-12ug-8081-7zz0386fbcb6",
"eventID":"8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType":"AwsApiCall",
"recipientAccountId":"831000000000"
}
```

Validation de conformité pour Resource Groups

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

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

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

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

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

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

Résilience dans les Resource Groups

AWS Resource Groupseffectue des sauvegardes automatisées sur les ressources de service internes. Ces sauvegardes ne sont pas configurables par l'utilisateur. Les sauvegardes sont chiffrées, tant au repos qu'en transit. Les Resource Groups stockent les données client dans Amazon DynamoDB.

L'infrastructure mondiale d'AWS est construite autour de zones de disponibilité et de Régions AWS. Les Régions AWSfournissent 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 de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Même une perte complète de groupes de ressources utilisateur n'entraînerait pas de perte de données client, car la plupart des données client sont répliquées surAWSZones de disponibilité (AZ). Si vous supprimez des groupes accidentellement, contactezAWS SupportCenter.

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

Sécurité de l'infrastructure dans Resource Groups

Il n'existe aucun autre moyen d'isoler le service ou le trafic réseau fournis par Resource Groups. Le cas échéant, utilisez AWS une isolation spécifique. Vous pouvez utiliser les Resource Groups API et la console VPC pour optimiser la confidentialité et la sécurité de l'infrastructure.

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

Vous utilisez des API appels AWS publiés pour accéder à Resource Groups 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.

Resource Groups ne prend pas en charge les politiques basées sur les ressources.

Éonnes pour les groupes de sécurité pour les Resource Groups sécurité pour

Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

- Utilisez le principe du moindre privilège pour accorder l'accès aux groupes. Les Resource Groups prennent en charge les autorisations au niveau des ressources. Accordez l'accès à des groupes spécifiques uniquement selon les besoins de certains utilisateurs. Évitez d'utiliser des astérisques dans les déclarations de politique qui attribuent des autorisations à tous les utilisateurs ou à tous les groupes. Pour plus d'informations sur le principe du moindre privilège, consultez la section Octroyer le moindre privilège dans le guide de l'utilisateur IAM.
- Gardez les informations privées hors des champs publics. Le nom d'un groupe est traité comme des métadonnées de service. Les noms des groupes ne sont pas cryptés. Ne mettez pas d'informations sensibles dans les noms de groupes. Les descriptions des groupes sont privées.

  Ne saisissez pas d'informations privées ou sensibles dans les clés ou les valeurs de balises.
- Utilisez l'autorisation basée sur le balisage chaque fois que cela est approprié. Les Resource Groups prennent en charge les autorisations basées sur des balises. Vous pouvez étiqueter des groupes, puis mettre à jour les politiques associées à vos principaux IAM, tels que les utilisateurs et les rôles, afin de définir leur niveau d'accès en fonction des balises appliquées à un groupe.

Pour plus d'informations sur l'utilisation de l'autorisation basée sur des balises, consultez la section Contrôle de l'accès auxAWS ressources à l'aide de balises de ressources dans le Guide de l'utilisateur IAM.

De nombreuxAWS services prennent en charge les autorisations basées sur des balises pour leurs ressources. Sachez que l'autorisation basée sur des balises peut être configurée pour les ressources des membres d'un groupe. Si l'accès aux ressources d'un groupe est restreint par des balises, les utilisateurs ou les groupes non autorisés risquent de ne pas être en mesure d'effectuer des actions ou des automatisations sur ces ressources. Par exemple, si une instance Amazon EC2 de l'un de vos groupes est balisée avec une clé de balise`Confidentiality` et une valeur de balise de`High`, et que vous n'êtes pas autorisé à exécuter des commandes sur les ressources balisées`Confidentiality:High`, les actions ou les automatisations que vous effectuez sur l'instance EC2 échoueront, même si les actions aboutissent pour d'autres ressources du groupe de ressources. Pour plus d'informations sur les services qui prennent en charge l'autorisation basée sur des balises pour leurs ressources, consultez la section AWSServices compatibles avec IAM dans le guide de l'utilisateur d'IAM.

Pour plus d'informations sur le développement d'une stratégie de balisage pour vosAWS ressources, consultez la section Stratégies deAWS balisage.

Quotas de service pour Resource Groups

Le tableau suivant décrit les quotas au sein de AWS Resource Groups (Resource Groups). Pour un quota ajustable, vous pouvez demander une augmentation dans la console Service Quotas.

Nom	Par défaut	Ajusta	Description
Groupes de ressources par compte	Chaque Région prise en charge : 100	Oui	Le nombre maximum de groupes de ressources que vous pouvez créer dans ce compte. Un groupe de ressources est un ensemble de AWS ressources qui répondent à des critères spécifiques.

AWS Resource Groups historique du document

Modification	Description	Date
Contenu mis à jour	Titres de sujets mis à jour et contenu réorganisé pour améliorer la lisibilité et la découvrabilité.	1er août 2024
Support pour un plus grand nombre de types de ressources	D'autres types de ressources sont désormais pris en charge par Resource Groups et Tag Editor.	30 mai 2024
Politiques AWS gérées mises à jour ResourceGroupsandTagEditorFullAccess et ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups a mis à jour deux politiques AWS gérées pour ajouter des AWS CloudFormation autorisations supplémentaires.	10 août 2023
Quotas de service Resource Groups	Vous pouvez désormais consulter les limites de quota de Resource Groups à l'aide de Service Quotas.	29 juin 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.	3 janvier 2023
Les informations de l'éditeur de balises ont été déplacées vers leur propre guide	La documentation de l'éditeur de balises a été supprimée de ce guide et déplacée vers le nouveau guide de l'utilisateur de l'éditeur de balises.	13 décembre 2022

Les groupes de ressources peuvent désormais inclure les ressources d'Amazon Keyspaces (pour Apache Cassandra)	AWS Resource Groups permet désormais d'inclure des ressources pour Amazon Keyspaces (pour Apache Cassandra) dans un groupe de ressources.	20 octobre 2022
Obsolète des types de ressources	Les types de ressources suivants ne sont plus pris en charge par Tag Editor : `AWS::RoboMaker::Robot` `AWS::RoboMaker::Fleet` ,, et`AWS::RoboMaker::DeploymentJob` .	17 mai 2022
Nouvelle politique AWS gérée - ResourceGroupsServiceRolePolicy	Resource Groups a ajouté une nouvelle politique AWS gérée dans AWS Identity and Access Management (IAM) pour soutenir le rôle lié aux services du service.	12 janvier 2022
Événements du cycle de vie du groupe	Resource Groups peut désormais générer des événements dans Amazon CloudWatch Events pour vous avertir lorsque des modifications sont apportées à vos groupes de ressources.	12 janvier 2022

Les groupes de ressources peuvent désormais être utilisés par Amazon VPC Network Access Analyzer pour surveiller le trafic réseau indésirable vers vos AWS ressources.	Vous pouvez l'utiliser AWS Resource Groups pour spécifier les sources et les destinations correspondant à vos exigences d'accès au réseau.	3 décembre 2021
Support supplémentaire pour les ressources du AWS Resilience Hub	AWS Resource Groups prend désormais en charge l'inclusion de ressources pour AWS Resilience Hub dans un groupe de ressources.	18 novembre 2021
Ajout de la prise en charge des ressources d'Amazon Pinpoint	AWS Resource Groups prend désormais en charge l'inclusion de ressources pour Amazon Pinpoint dans un groupe de ressources.	11 novembre 2021
Ajout de la prise en charge des groupes de ressources configurés et gérés par AppRegistry	AWS Resource Groups prend désormais en charge les groupes de ressources qui contiennent des configurations de service pour les ressources des applications que vous créez à l'aide de AWS Service Catalog AppRegistry. Pour plus d'informations, consultez la section Configurations des services dans la AWS Resource Groups APIréférence.	15 septembre 2021

Support supplémentaire pour les ressources d'Amazon OpenSearch Service	AWS Resource Groups prend désormais en charge l'inclusion de ressources pour Amazon OpenSearch Service dans un groupe de ressources.	11 août 2021
Ajout du support pour les ressources de AWS Braket	AWS Resource Groups prend désormais en charge l'inclusion de ressources pour AWS Braket dans un groupe de ressources.	30 Juin 2021
Ajout de la prise en charge des ressources d'Amazon EMR Containers	AWS Resource Groups prend désormais en charge l'inclusion de ressources pour EMR les conteneurs Amazon dans un groupe de ressources.	27 avril 2021
Support supplémentaire pour les ressources de AWS services supplémentaires	AWS Resource Groups prend désormais en charge l'inclusion de ressources pour les services suivants dans un groupe de ressources : Amazon CodeGuru Reviewer, Amazon Elastic Inference, Amazon Forecast, Amazon Fraud Detector et Service Quotas.	25 février 2021
Ajout d'un chapitre sur la sécurité et la conformité.	Explique comment Resource Groups protège vos informations et se conforme aux normes réglementaires.	30 juillet 2020

Ajout de la prise en charge des groupes de ressources configurés pour les AWS services	Vous pouvez désormais créer des groupes de ressources associés à un AWS service et qui configurent la manière dont le service peut interagir avec les ressources du groupe. Dans cette première version de cette fonctionnalité, vous pouvez créer un groupe de ressources contenant les réservations de EC2 capacité Amazon, puis lancer des EC2 instances Amazon dans le groupe. Si la capacité d'une ou de plusieurs réservations du groupe correspond à celle de votre instance, cette instance utilise la réservation. Si l'instance ne correspond à aucune réservation disponible dans le groupe, elle est lancée en tant qu'instance à la demande. Pour plus d'informations, consultez la section Travailler avec des groupes de réservation de capacité dans le guide de EC2 l'utilisateur Amazon.	29 juillet 2020
Ajout de la prise en charge AWS IoT Greengrass des ressources.	D'autres types de ressources sont désormais pris en charge par AWS Resource Groups et Tag Editor.	25 mars 2020

Afficher les données d'exploitation pour AWS Resource Groups	Dans la AWS Systems Manager console, la AWS Resource Groups page affiche les données d'opérations d'un groupe sélectionné dans quatre onglets : Détails, Config, CloudTrail, OpsItems. Ces onglets ne sont pas disponibles lorsque vous consultez un groupe dans la console Resource Groups. Les informations de ces onglets peuvent vous aider à comprendre quelles ressources au sein d'un groupe sont conformes et fonctionnent correctement, et quelles ressources demandent une action. Si vous devez agir sur une ressource, vous pouvez utiliser les runbooks d'automatisation Systems Manager pour effectuer des tâches courantes de maintenance et de dépannage. Pour plus d'informations, consultez la section Affichage des données relatives aux opérations AWS Resource Groups dans le Guide de AWS Systems Manager l'utilisateur.	16 mars 2020

Vérifier la conformité avec les politiques relatives aux balises	Une fois que vous avez créé et associé des politiques de balises aux comptes à l'aide de celles-ci AWS Organizat ions, vous pouvez trouver des balises non conformes sur les ressources des comptes de votre organisation.	26 novembre 2019
Support pour un plus grand nombre de types de ressource s	D'autres types de ressources sont désormais pris en charge par AWS Resource Groups et Tag Editor.	4 octobre 2019
Nouveaux types de ressource s pris en charge par AWS Resource Groups	Davantage de types de ressources sont désormais pris en charge par AWS Resource Groups, en particuli er pour les groupes basés sur une AWS CloudFormation pile.	5 août 2019
Nouveaux types de ressource s pris en charge par AWS Resource Groups	Amazon API Gateway RESTAPIs, Amazon CloudWatch Events events et Amazon SNS topics sont désormais des types de ressources pris en charge dans AWS Resource Groups.	27 juin 2019
L'éditeur de balises permet désormais de rechercher des ressources non étiquetées	Vous pouvez désormais rechercher des ressource s dans l'éditeur de balises auxquelles aucune valeur de balise n'est appliquée pour une clé de balise spécifique.	18 juin 2019

Nouveaux types de ressources pris en charge par AWS Resource Groups et Tag Editor	Plus de 50 nouveaux types de ressources ont été ajoutés AWS Resource Groups et pris en charge par Tag Editor.	6 juin 2019
AWS Resource Groups et la console Tag Editor quitte la AWS Systems Manager console	La console AWS Resource Groups and Tag Editor est désormais indépendante de la console Systems Manager. Bien que vous puissiez toujours trouver des pointeurs vers la AWS Resource Groups console dans la barre de navigation de gauche de Systems Manager, vous pouvez ouvrir la console Resource Groups and Tag Editor directement depuis le menu déroulant en haut à gauche du AWS Management Console.	5 juin 2019
Nouvelles fonctionnalités d'autorisation et de contrôle d'accès de Resource Groups	Resource Groups prend désormais en charge les politiques basées sur l'action, les autorisations au niveau des ressources et les autorisations basées sur des balises.	24 mai 2019

Les anciens outils Resource Groups et Tag Editor ne sont plus disponibles	Les mentions de Resource Groups et de Tag Editor anciens, classiques ou anciens ont été supprimée s ; ces outils ne sont plus disponibles dans AWS. Utilisez AWS Resource Groups plutôt un éditeur de balises.	14 mai 2019
L'éditeur de balises prend désormais en charge le balisage des ressources dans plusieurs régions	Tag Editor vous permet désormais de rechercher et de gérer des balises des ressources dans plusieurs régions, avec votre région actuelle ajoutée aux requêtes de ressources par défaut.	2 mai 2019
L'éditeur de balises prend désormais en charge l'exporta tion des résultats des requêtes vers un CSV	Vous pouvez exporter les résultats d'une requête sur la page Rechercher des ressources à étiqueter dans un fichier au CSV format. Une nouvelle colonne Région est présente dans les résultats des requêtes de Tag Editor. Tag Editor vous permet désormais de rechercher des ressources qui ont des valeurs vides pour une clé de balise spécifique. Baliser des valeurs de clé à remplissage automatique à mesure que vous tapez une valeur unique parmi des clés existantes.	2 avril 2019

L'éditeur de balises permet désormais d'ajouter tous les types de ressources à une requête	Vous pouvez appliquer des balises jusqu'à 20 types de ressources individuelles en une seule opération, ou choisir All resource types (Tous les types de ressource) pour interroger tous les types de ressources dans une région. Le remplissage automatique a été ajouté au champ Tag key (Clé de balise) d'une requête, pour aider à activer des clés de balise cohérentes entre les ressource s. Si les changements de balise échouent sur certaines ressources, vous pouvez les relancer uniquement pour les ressources pour lesquelles les ils ont échoué.	19 mars 2019
L'éditeur de balises prend désormais en charge plusieurs types de ressources dans une recherche	Vous pouvez appliquer des balises à 20 types de ressources maximum en une seule opération. Vous pouvez également choisir les colonnes qui sont présentées dans les résultats de la recherche, y compris les colonnes pour chaque clé de balise unique trouvée dans vos résultats de recherche ou les ressource s sélectionnées à partir des résultats.	26 février 2019

Documentation ajoutée pour le nouvel éditeur de balises	La section « Utilisation de l'éditeur de balises » décrit comment utiliser la nouvelle expérience de console de l'éditeur de AWS balises.	13 février 2019
Nouveaux types de ressources pris en charge pour les groupes dans Resource Groups	Ajout de nouveaux types de ressources qui sont désormais pris en charge dans Resource Groups.	4 février 2019
Expérience utilisateur améliorée pour l'ajout de balises aux requêtes Resource Groups basées sur des balises	Modifications mineures à l'expérience utilisateur de la console pour ajouter des balises dans une requête basée sur des balises.	le 17 décembre 2018
AWS CloudFormation support de requêtes basé sur une pile ajouté à Resource Groups	Vous pouvez créer des groupes de ressources dans lesquels la requête est basée sur une AWS CloudFormation pile. Une fois que vous avez choisi une pile, vous pouvez choisir les types de ressource de la pile que vous souhaitez faire apparaître dans votre requête de groupe.	13 novembre 2018
Resource Groups et CloudTrail	Resource Groups propose désormais une AWS CloudTrail assistance. Vous pouvez consulter et utiliser les journaux de tous les API appels reçus par Resource Groups CloudTrail.	29 juin 2018

- APIversion : 27/11/2017

- Dernière mise à jour de la documentation : 24 septembre 2019

Mises à jour antérieures

Le tableau ci-après décrit des modifications importantes apportées dans chaque version du Guide de l'utilisateur AWS Resource Groups avant juin 2018.

Modification	Description	Date
Première version	Sortie initiale de la prochaine génération de AWS Resource Groups	29 novembre 2017

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.