Guide de l'utilisateur

Identification AWS Éditeur de ressources et de balises

Version 1.0

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Identification AWS Éditeur de ressources et de balises: Guide de l’utilisateur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service qui n’appartient pas à Amazon, de toute manière susceptible de créer une confusion chez les clients ou de toute manière dénigrant ou discréditant Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que Tag Editor ? 1
Méthodes de balisage 2
En savoir plus 3
Bonnes pratiques et stratégies 3
Bonnes pratiques 3
Bonnes pratiques en matière de dénomination des balises 4
Stratégies de balisage courantes 6
Catégories de balisage 8
Prise en main 10
Conditions préalables 11
Inscrivez-vous pour un Compte AWS 11
Créer des ressources 11
Configuration d'autorisations 11
Autorisations pour des services individuels 12
Autorisations requises pour utiliser la console Tag Editor 12
Octroi d'autorisations pour l'utilisation de l'éditeur de balises 15
Autorisation et contrôle d'accès basés sur des balises 16
Trouver des ressources à étiqueter 18
Afficher et modifier les balises existantes pour une ressource sélectionnée 20
Exporter les résultats vers un fichier .csv 21
Gestion des tags 23
Ajouter des balises aux ressources sélectionnées 24
Modifier les balises des ressources sélectionnées 25
Supprimer les balises des ressources sélectionnées 27
Utilisation de balises dans les politiques IAM 29
Contrôle d'accès basé sur les balises et les attributs 29
Clés de condition liées aux balises 30
Exemples de politiques IAM utilisant des balises 30
AWS Organizations politiques relatives aux balises 33
Conditions préalables et autorisations 33
Conditions préalables à l'évaluation de la conformité aux politiques relatives aux balises 33
Autorisations pour évaluer la conformité d'un compte 34
Autorisations pour évaluer la conformité à l'échelle de l'organisation 35
Politique relative aux compartiments Amazon S3 pour le stockage des rapports 38

Évaluation de la conformité d'un compte 39
Évaluation de la conformité à l'échelle de l'entreprise 42
Surveillance des modifications des balises 45
Les modifications de balises génèrent des EventBridge événements 45
Lambda et sans serveur 47
Tutoriel de surveillance 47
Étape 1. Créer la fonction Lambda 49
Étape 2. Configurer les autorisations IAM requises 52
Étape 3. Effectuez un test préliminaire de votre fonction Lambda 54
Étape 4 : Créez la EventBridge règle qui lance la fonction 57
Étape 5. Testez la solution complète 58
Résumé du didacticiel 60
Résolution des problèmes de modification des balises 61
Réessayer les modifications de balises qui ont échoué 62
Sécurité 63
Protection des données 64
Chiffrement des données 65
Confidentialité du trafic inter-réseau 65
Gestion des identités et des accès 65
Public ciblé 66
Authentification par des identités 66
Gestion de l'accès à l'aide de politiques 67
Comment fonctionne Tag Editor avec IAM 70
Exemples de politiques basées sur l'identité 73
Résolution des problèmes 78
Journalisation et surveillance 79
CloudTrail Integration 79
Validation de conformité 82
Résilience 82
Sécurité de l'infrastructure 83
Quotas du service Tag Editor 84
Historique de la documentation 87
..... xci

Qu'est-ce que Tag Editor ?

L'éditeur de balises vous permet de gérer efficacement les balises. 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. Les exemples de ressources incluent une instance Amazon Elastic Compute Cloud (Amazon EC2), un bucket Amazon Simple Storage Service (Amazon S3) ou un secret in. AWS Secrets Manager

> **Important**
>
> Ne stockez pas d'informations personnelles 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.

Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères.

Chaque balise se compose de deux parties :

- Une clé de balise (par exemple, `CostCenter`, `Environment` ou `Project`). Les touches de tag distinguent les majuscules et minuscules.
- Une valeur de balise (par exemple, `111122223333` ou `Production`). Les valeurs de balise sont sensibles à la casse, tout comme les clés de balise.

> **Note**
>
> Bien que les clés de balise distinguent les majuscules et minuscules, IAM propose des validations supplémentaires pour les ressources IAM afin d'empêcher l'application de clés de balise dont le boîtier ne diffère que par le boîtier. Nous vous recommandons de ne pas utiliser de clés dont le boîtier diffère uniquement. Reportez-vous à la section Tags pour les ressources IAM pour plus d'informations.

Méthodes de balisage des ressources

Il existe trois méthodes pour ajouter des balises à vos AWS ressources :

- Service AWS Fonctionnement de l'API — Les opérations d'API de balisage sont prises en charge directement par un Service AWS. Pour découvrir les fonctionnalités de balisage proposées par chaque Service AWS service, consultez la documentation du service dans l'index de la AWS documentation.
- Console de l'éditeur de balises : certains services prennent en charge le balisage à l'aide de la console de l'éditeur de balises.
- API de balisage Resource Groups — La plupart des services prennent également en charge le balisage à l'aide du. AWS Resource Groups Tagging API

> **Note**
>
> Vous pouvez également utiliser AWS Service Catalog TagOptions Library pour gérer facilement les balises des produits approvisionnés. A TagOptionest une paire clé-valeur gérée dans Service Catalog. Il ne s'agit pas d'un AWS tag, mais sert de modèle pour créer un AWS tag basé sur le TagOption.

Vous pouvez étiqueter les ressources pour tous les services générateurs de coûts dans AWS. Pour les services suivants, AWS recommande une alternative plus récente Services AWS qui prend en charge le balisage afin de mieux répondre aux cas d'utilisation des clients.

Amazon Cloud Directory	Amazon CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon Glacier Direct	Amazon SimpleDB
Gestionnaire WorkSpaces d'applications Amazon	AWS DeepLens	

En savoir plus

Cette page fournit des informations générales sur le balisage des AWS ressources. Pour plus d'informations sur le balisage des ressources dans un AWS service donné, consultez sa documentation. Voici également quelques sources d'information fiables sur le balisage :

- Pour plus d'informations à ce sujet AWS Resource Groups Tagging API, consultez le Guide de référence de l'API Resource Groups Tagging.
- Pour plus d'informations sur les fonctionnalités de balisage Service AWS fournies par chacun d'entre eux, consultez la documentation du service dans l'index de la AWS documentation.
- Pour plus d'informations sur l'utilisation de balises dans les politiques IAM afin de contrôler qui peut consulter et interagir avec vos AWS ressources, consultez la section Contrôle de l'accès aux utilisateurs et aux rôles IAM à l'aide de balises dans le Guide de l'utilisateur IAM.

Bonnes pratiques et stratégies

Ces sections fournissent des informations sur les meilleures pratiques et stratégies relatives au balisage de vos AWS ressources et à l'utilisation de Tag Editor.

Bonnes pratiques en matière de balisage

Lorsque vous créez une stratégie de balisage pour les AWS ressources, suivez les meilleures pratiques :

- N'ajoutez pas de données d'identification personnelle (PII) ou d'autres informations confidentielles ou sensibles dans les étiquettes. Les tags sont accessibles à de nombreux AWS services, y compris la facturation. Les étiquettes ne sont pas destinées à être utilisées pour des données privées ou sensibles.
- Utilisez un format standardisé et sensible à la casse pour les balises et appliquez-le de manière cohérente à tous les types de ressources.
- Optez pour des directives de balisage qui prennent en charge plusieurs objectifs, comme la gestion du contrôle d'accès aux ressources, le suivi des coûts, l'automatisation et l'organisation.
- Utilisez des outils automatisés pour gérer les balises de ressources. L'éditeur de balises et l'API Resource Groups Tagging permettent le contrôle programmatique des balises, ce qui facilite la gestion, la recherche et le filtrage automatiques des balises et des ressources.
- Utilisez trop de balises plutôt que trop peu.

- N'oubliez pas qu'il est facile de modifier les étiquettes pour s'adapter aux besoins en évolution de l'entreprise, mais tenez compte des conséquences des changements futurs. Par exemple, la modification des balises de contrôle d'accès signifie que vous devez également mettre à jour les stratégies qui font référence à ces balises et contrôler l'accès à vos ressources.
- Vous pouvez appliquer automatiquement les normes de balisage que votre organisation choisit d'adopter en créant et en déployant des politiques de balisage en utilisant AWS Organizations. Les politiques de balisage vous permettent de définir des règles de balisage qui définissent des noms de clé valides et des valeurs valides pour chaque clé. Vous pouvez choisir de surveiller uniquement, ce qui vous permet d'évaluer et de nettoyer vos balises existantes. Une fois que vos balises sont conformes aux normes que vous avez choisies, vous pouvez activer l'application dans les politiques relatives aux balises afin d'empêcher la création de balises non conformes. Pour en savoir plus, consultez Politiques de balises dans le Guide de l'utilisateur AWS Organizations .

Bonnes pratiques en matière de dénomination des balises

Voici quelques bonnes pratiques et conventions de dénomination que nous vous recommandons d'utiliser avec vos balises. Reportez-vous à la section Attribution de noms dans le guide de l'utilisateur IAM pour plus d'informations.

Un certain nombre de balises sont prédéfinies AWS ou créées automatiquement par divers Services AWS. De nombreuses balises AWS générées utilisent des noms de clé qui sont tous en minuscules, avec des tirets séparant les mots dans le nom, et des préfixes suivis de deux points pour identifier le service source de la balise. Par exemple, consultez ce qui suit :

- `aws:ec2spot:fleet-request-id`est une balise qui identifie la demande d'instance Amazon EC2 Spot qui a lancé l'instance.
- `aws:cloudformation:stack-name`est une balise qui identifie la CloudFormation pile qui a créé la ressource.
- `elasticbeanstalk:environment-name`est une balise qui identifie l'application qui a créé la ressource.

Pensez à nommer vos tags en respectant les règles suivantes :

- Utilisez tous les mots en minuscules.
- Utilisez des tirets pour séparer les mots.
- Utilisez un préfixe suivi de deux points pour identifier le nom de l'organisation ou son nom abrégé.

Par exemple, pour une société fictive nommée AnyCompany, vous pouvez définir des balises telles que :

- `anycompany:cost-center`pour identifier le code interne du centre de coûts.
- `anycompany:environment-type`pour déterminer s'il s'agit d'un environnement de développement, de test ou de production.
- `anycompany:application-id`pour identifier l'application pour laquelle la ressource a été créée.

Le préfixe garantit que les balises sont clairement reconnaissables telles que définies par votre organisation et AWS non par un outil tiers que vous pourriez utiliser. L'utilisation de minuscules et de traits d'union pour les séparateurs évite toute confusion quant à l'utilisation de majuscules pour le nom d'une balise. Par exemple, `anycompany:project-id`est plus simple à mémoriser que `ANYCOMPANY:ProjectID`, `anycompany:projectID` ou`Anycompany:ProjectId`.

Limites et exigences de dénomination des balises

Les exigences de base suivantes s'appliquent aux balises en matière de dénomination et d'utilisation :

- Chaque ressource peut avoir un maximum de 50 balises créées par l'utilisateur.
- Les balises créées par le système qui commencent par `aws:` sont réservées à l'utilisation d' AWS et ne sont pas prises en compte dans cette limite. Vous ne pouvez pas modifier ou supprimer une balise commençant par le préfixe `aws:`.
- Pour chaque ressource, chaque clé d'identification doit être unique, et chaque clé d'identification peut avoir une seule valeur.
- La clé de balise doit comporter au minimum 1 et au maximum 128 caractères Unicode en UTF-8.
- La valeur de balise doit être au minimum de 0 et au maximum de 256 caractères Unicode en UTF-8.
- Les caractères autorisés peuvent varier en fonction AWS du service. Pour plus d'informations sur les caractères que vous pouvez utiliser pour étiqueter les ressources d'un AWS service donné, consultez sa documentation. En général, les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : _ . : / = + - @.
- Les clés et les valeurs des balises distinguent les majuscules et minuscules. La bonne pratique consiste à choisir une politique pour mettre des balises en majuscule et mettre en œuvre cette politique de manière cohérente sur tous les types de ressources. Par exemple, décidez si vous souhaitez utiliser `Costcenter`, `costcenter` ou `CostCenter`, et utilisez la même convention

pour toutes les balises. Évitez d'utiliser des balises avec une incohérence de traitement de cas similaires.

Stratégies de balisage courantes

Utilisez les stratégies de balisage suivantes pour identifier et gérer les ressources AWS .

Table des matières

- Balises pour l'organisation des ressources
- Balises pour la répartition des coûts
- Balises pour l'automatisation
- Balises pour le contrôle d'accès
- Gouvernance du balisage

Balises pour l'organisation des ressources

Les balises sont un bon moyen d'organiser AWS les ressources dans le Console de gestion AWS. Vous pouvez configurer les balises pour qu'elles s'affichent avec les ressources, et rechercher et filtrer par balise. Ce Groupes de ressources AWS service vous permet de créer des groupes de AWS ressources basés sur une ou plusieurs balises ou parties de balises. Vous pouvez également créer des groupes en fonction de leur occurrence dans une AWS CloudFormation pile. À l'aide des Groupes de ressources et de l'Éditeur de balises, vous pouvez regrouper et afficher les données des applications composées de plusieurs services, ressources et régions en un seul endroit.

Balises pour la répartition des coûts

AWS Cost Explorer et les rapports de facturation détaillés vous permettent de ventiler AWS les coûts par étiquette. Généralement, vous utilisez des balises commerciales telles que l' center/business unité de coût, le client ou le projet pour associer AWS les coûts aux dimensions traditionnelles de répartition des coûts. Cependant, un rapport de répartition des coûts peut inclure n'importe quelle balise. Cela vous permet d'associer facilement des coûts à des aspects techniques ou de sécurité, tels que des applications, des environnements ou des programmes de conformité spécifiques.

Pour certains services, vous pouvez utiliser une `createdBy` balise AWS générée à des fins de répartition des coûts, afin de prendre en compte les ressources qui pourraient autrement ne pas être classées. La balise `createdBy` n'est disponible que pour les services et les ressources AWS

pris en charge. Sa valeur contient des données associées à des événements d'API ou de console spécifiques. Pour plus d'informations, veuillez consulter la section Balises de répartition des coûts générées par AWS dans le Guide de l'utilisateur AWS Billing and Cost Management .

Balises pour l'automatisation

Les balises spécifiques aux ressources ou aux services sont souvent utilisées pour filtrer les ressources pendant les activités d'automatisation. Les balises d'automatisation sont utilisées pour accepter ou refuser des tâches automatisées, ou pour identifier des versions spécifiques de ressources à archiver, mettre à jour ou supprimer. Par exemple, vous pouvez exécuter des scripts automatisés `start` ou `stop` qui désactivent les environnements de développement en dehors des heures ouvrables afin de réduire les coûts. Dans ce scénario, les balises d'instance Amazon Elastic Compute Cloud (Amazon EC2) constituent un moyen simple d'identifier les instances afin de refuser cette action. Pour les scripts qui détectent et suppriment des instantanés Amazon EBS périmés ou permanents, les balises d'instantané peuvent ajouter une dimension supplémentaire aux critères de recherche. out-of-date

Balises pour le contrôle d'accès

Les politiques IAM prennent en charge les conditions basées sur des balises, ce qui vous permet de restreindre les autorisations IAM en fonction de balises ou de valeurs spécifiques. Par exemple, les autorisations d'utilisateur ou de rôle IAM peuvent inclure des conditions visant à limiter les appels d' EC2 API à des environnements spécifiques (tels que le développement, les tests ou la production) en fonction de leurs balises. La même stratégie peut être utilisée pour limiter les appels d'API à des réseaux Amazon Virtual Private Cloud (Amazon VPC) spécifiques. La prise en charge des autorisations IAM au niveau des ressources basées sur des balises est spécifique au service. Lorsque vous utilisez des conditions basées sur des balises pour le contrôle d'accès, assurez-vous de définir et de restreindre qui peut modifier les balises. Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès des API aux AWS ressources, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Gouvernance du balisage

Une stratégie de balisage efficace utilise des balises standardisées et les applique de manière cohérente et programmatique à toutes les ressources. AWS Vous pouvez utiliser des approches réactives et proactives pour gérer les balises dans votre AWS environnement.

- La gouvernance réactive permet de trouver les ressources qui ne sont pas correctement étiquetées à l'aide d'outils tels que l'API Resource Groups Tagging et de scripts personnalisés. AWS Config

Rules Pour rechercher des ressources manuellement, vous pouvez utiliser l'Éditeur de balises et des rapports de facturation détaillés.

- La gouvernance proactive utilise des outils tels que Service Catalog CloudFormation, les politiques de balises ou les autorisations au AWS Organizations niveau des ressources IAM pour garantir que les balises standardisées sont appliquées de manière cohérente lors de la création des ressources.

  Par exemple, vous pouvez utiliser la CloudFormation `Resource Tags` propriété pour appliquer des balises aux types de ressources. Dans Service Catalog, vous pouvez ajouter des balises de portefeuille et de produit qui sont combinées et appliquées automatiquement à un produit lorsqu'il est lancé. Des formes plus rigoureuses de gouvernance proactive comprennent des tâches automatisées. Par exemple, vous pouvez utiliser l'API de balisage des groupes de ressources pour rechercher les balises d'un environnement AWS ou exécuter des scripts pour mettre en quarantaine ou supprimer des ressources mal balisées.

Catégories de balisage

Les entreprises les plus efficaces dans leur utilisation des balises créent généralement des groupes de balises pertinents pour l'entreprise afin d'organiser leurs ressources selon des dimensions techniques, commerciales et de sécurité. Les entreprises qui utilisent des processus automatisés pour gérer leur infrastructure incluent également des balises supplémentaires spécifiques à l'automatisation.

Balises techniques	Balises pour l'automatisation	Balises d'activités	Balises de sécurité
• Nom – Identifie les ressources individuelles • ID de l'application – Identifie les ressources liées à une application spécifique • Rôle d'application – Décrit la fonction d'une ressource	• Date/Heure – Identifie la date ou l'heure de démarrage, d'arrêt, de suppression ou de rotation d'une ressource • Option/désactivation – Indique si une ressource doit être incluse dans une	• Projet – Identifie les projets pris en charge par la ressource • Propriétaire – Identifie qui est responsable de la ressource • Centre de coût/unité commerciale – Identifie le	• Confidentialité – Identifiant pour le niveau spécifique de confidentialité des données pris en charge par une ressource. • Conformité – Identifiant pour les charges de travail qui doivent

Balises techniques	Balises pour l'automatisation	Balises d'activités	Balises de sécurité
particulière (comme un serveur web, un agent de messages, une base de données) • Cluster – Identifie les batteries de ressources qui partagent une configuration commune et exécutent une fonction spécifique pour une application • Environnement – Différencie les ressources de développement, de test et de production • Version – Aide à différencier les versions des ressources ou des applications	activité automatisée telle que le démarrage, l'arrêt ou le redimensionnement des instances • Sécurité – Détermine les exigences, telles que le chiffrement ou l'activation des journaux de flux Amazon VPC ; identifiez les tables de routage ou les groupes de sécurité nécessitant un contrôle supplémentaire	centre de coûts ou l'unité commerciale associé à une ressource, généralement pour l'allocation et le suivi des coûts • Client – Identifie un client spécifique servi par un groupe particulier de ressources	respecter des exigences de conformité spécifiques

Commencer à utiliser Tag Editor

> **Important**
>
> Ne stockez pas de données d'identification personnelle (PII) ni 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 ajouter des balises à plusieurs ressources à la fois, ou modifier ou supprimer des balises, utilisez l'éditeur de balises. Avec Tag Editor, vous pouvez rechercher les ressources que vous souhaitez baliser, puis gérer les balises des ressources de vos résultats de recherche.

Pour démarrer Tag Editor

1. Connectez-vous à la Console de gestion AWS.
2. Effectuez l'une des étapes suivantes :
   - Choisissez Services. Ensuite, sous Management & Governance, choisissez Resource Groups & Tag Editor. Dans le volet de navigation de gauche, choisissez Tag Editor.
   - Utilisez le lien direct : console AWS Tag Editor.

Des balises ne sont pas appliquées à toutes les ressources. Pour plus d'informations sur les ressources prises en charge par l'éditeur de balises, consultez la colonne de balisage de l'éditeur de balises sous Types de ressources pris en charge dans le guide de Groupes de ressources AWS l'utilisateur. Si un type de ressource que vous souhaitez baliser n'est pas pris en charge, faites-le AWS savoir en choisissant Feedback dans le coin inférieur gauche de la fenêtre de console.

Pour plus d'informations sur les autorisations et les rôles nécessaires pour baliser les ressources, consultez Configuration d'autorisations.

Rubriques

- Conditions préalables à l'utilisation de Tag Editor
- Configuration d'autorisations

Conditions préalables à l'utilisation de Tag Editor

Avant de commencer à étiqueter vos ressources, assurez-vous de disposer d'une ressource active Compte AWS avec les ressources existantes et des droits appropriés pour étiqueter les ressources et créer des groupes.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Créer des ressources

Inscrivez-vous pour un Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Pour plus d'informations sur la création d'un Compte AWS, voir Getting started with an Compte AWS dans le Guide de Gestion de compte AWS référence.

Créer des ressources

Vous devez avoir des ressources dans votre balise Compte AWS to. Pour plus d'informations sur les types de ressources pris en charge, consultez la colonne de balisage de l'éditeur de balises sous Types de ressources pris en charge dans le guide de Groupes de ressources AWS l'utilisateur.

Configuration d'autorisations

Pour utiliser pleinement l'éditeur de balises, vous aurez peut-être besoin d'autorisations supplémentaires pour étiqueter les ressources ou pour voir les clés et les valeurs des balises d'une ressource. Ces autorisations appartiennent aux catégories suivantes :

- 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.

Si vous êtes administrateur, vous pouvez fournir des autorisations à vos utilisateurs en créant des politiques via le service Gestion des identités et des accès AWS (IAM). Vous créez d'abord des rôles, des utilisateurs ou des groupes IAM, puis vous appliquez les politiques avec les autorisations dont ils ont besoin. Pour plus d'informations sur la création et l'attachement de politiques IAM, consultez la section Utilisation des politiques.

Autorisations pour des services individuels

> **Important**
>
> Cette section décrit les autorisations requises si vous souhaitez baliser des ressources provenant d'autres consoles de AWS service et API.

Pour ajouter des balises à une ressource, vous devez disposer des autorisations nécessaires pour le service auquel appartient la ressource. Par exemple, pour baliser des instances Amazon EC2, vous devez être autorisé à effectuer les opérations de balisage dans l'API de ce service, telles que l'opération Amazon EC2. CreateTags

Autorisations requises pour utiliser la console Tag Editor

Pour utiliser la console Tag Editor pour répertorier et étiqueter les ressources, les autorisations suivantes doivent être ajoutées à la déclaration de politique d'un utilisateur dans IAM. Vous pouvez soit ajouter des politiques AWS gérées qui sont maintenues et mises à jour par AWS, soit créer et gérer votre propre politique personnalisée.

Utilisation AWS politiques gérées pour les autorisations de l'éditeur de balises

L'éditeur de balises prend en charge les politiques AWS gérées suivantes que vous pouvez utiliser pour fournir un ensemble prédéfini d'autorisations à vos utilisateurs. Vous pouvez associer ces politiques gérées à n'importe quel rôle, utilisateur ou groupe comme vous le feriez pour toute autre politique que vous créez.

ResourceGroupsandTagEditorReadOnlyAccess

Cette politique accorde au rôle IAM ou à l'utilisateur associé l'autorisation d'appeler les opérations en lecture seule pour les deux Groupes de ressources AWS et pour 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. Pour en savoir plus, consultez la note importante suivante.

ResourceGroupsandTagEditorFullAccess

Cette politique accorde au rôle IAM 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. Pour en savoir plus, consultez la note importante suivante.

Important

Les deux politiques précédentes accordent l'autorisation d'appeler les opérations de l'éditeur de balises et d'utiliser la console de l'éditeur de balises. Cependant, vous devez également disposer des autorisations non seulement pour appeler 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 :

- La politique AWS gérée ReadOnlyAccessaccorde des autorisations aux opérations en lecture seule pour les ressources de chaque service. AWS met automatiquement cette politique à jour au Services AWS fur et à mesure qu'elles sont disponibles.
- De nombreux services fournissent des politiques AWS gérées en lecture seule spécifiques à un service que vous pouvez utiliser pour limiter l'accès aux seules ressources fournies par ce service. Par exemple, Amazon EC2 fournit. AmazonEC2ReadOnlyAccess
- Vous pouvez créer votre propre politique qui n'accorde l'accès qu'aux opérations spécifiques en lecture seule 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.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": [
                "arn:aws:ec2:us-east-1:444455556666:*",
                "arn:aws:s3:::amzn-s3-demo-bucket2"
                ]
```

```
        }
    ]
}
```

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. Cela nécessite une politique distincte qui s'applique aux utilisateurs concernés et qui autorise l'accès. L'exemple de politique suivant refuse ensuite l'accès aux ressources spécifiques répertoriées par l'Amazon Resource Name (ARN).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [ "tag:*" ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance:*",
                "arn:aws:s3:::amzn-s3-demo-bucket3"
             ]
        }
    ]
}
```

Ajouter manuellement les autorisations de l'éditeur de balises

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

- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **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.

Octroi d'autorisations pour l'utilisation de l'éditeur de balises

Pour ajouter une politique d'utilisation Groupes de ressources AWS et un éditeur de balises à un rôle, procédez comme suit.

1. Ouvrez la console IAM sur la page Rôles.
2. Trouvez le rôle auquel vous souhaitez accorder les autorisations de Tag Editor. Choisissez le nom du rôle pour ouvrir la page de résumé du rôle.
3. Sous l'onglet Autorisations, sélectionnez Ajouter des autorisations.
4. Choisissez Attach existing policies directly (Attacher directement les politiques existantes).
5. Choisissez Create Policy (Créer une politique).
6. Dans l'onglet JSON, collez la déclaration de stratégie suivante.

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
```

```
        "tag:getTagValues",
        "resource-explorer:*",
        "resource-groups:SearchResources",
        "resource-groups:ListResourceTypes"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Cet exemple de déclaration de politique accorde des autorisations pour effectuer uniquement des actions de l'éditeur de balises.

7. Sélectionnez Next: Tags (Suivant : Balises), puis Next: Review (Suivant : Vérification).
8. Entrez le nom et la description de la nouvelle politique. Par exemple, **`AWSTaggingAccess`**.
9. Choisissez Create Policy (Créer une politique).

Maintenant que la politique est enregistrée dans IAM, vous pouvez l'associer à d'autres principes, tels que des rôles, des groupes ou des utilisateurs. Pour plus d'informations sur la façon d'ajouter une politique à un principal, consultez la section Ajouter et supprimer des autorisations d'identité IAM dans le guide de l'utilisateur IAM.

Autorisation et contrôle d'accès basés sur des balises

Services AWS soutenez les éléments suivants :

- Action-based politiques : par exemple, vous pouvez créer une politique qui permet aux utilisateurs d'effectuer `GetTagKeys` des `GetTagValues` opérations, mais pas d'autres.
- Resource-level autorisations dans les politiques — De nombreux services prennent en charge l'utilisation d'ARN pour spécifier des ressources individuelles dans la politique.
- Autorisation basée sur des balises — De nombreux services prennent 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 d'accéder pleinement à un groupe qui possède le même tag que les utilisateurs. Pour plus d'informations, voir À quoi sert ABAC ? AWS dans le guide de Gestion des identités et des accès AWS l'utilisateur.

- Informations d'identification temporaires : les utilisateurs peuvent assumer un rôle dans le cadre d'une politique autorisant les opérations de l'éditeur de balises.

L'éditeur de balises n'utilise aucun rôle lié à un service.

Pour plus d'informations sur la façon dont Tag Editor s'intègre à Gestion des identités et des accès AWS (IAM), consultez les rubriques suivantes du guide de l'Gestion des identités et des accès AWS utilisateur :

- AWS services qui fonctionnent avec IAM
- Actions, ressources et clés de condition pour Tag Editor
- Contrôle de l'accès aux AWS ressources à l'aide de politiques

Trouver des ressources à étiqueter

Avec Tag Editor, vous créez une requête pour trouver des ressources dans une ou plusieurs Régions AWS ressources disponibles pour le balisage. Vous pouvez choisir jusqu'à 20 types de ressources individuelles, ou créer une requête sur All resource types (Tous les types de ressources). Votre requête peut inclure des ressources qui ont déjà des balises ou des ressources qui n'en ont pas. Pour plus d'informations, consultez la colonne de balisage de l'éditeur de balises sous Types de ressources pris en charge dans le guide de l'Groupes de ressources AWS utilisateur.

Après avoir trouvé des ressources à baliser, vous pouvez utiliser Tag Editor pour ajouter des balises, ou afficher, modifier ou supprimer des balises.

Pour rechercher des ressources à baliser

1. Ouvrez la console Tag Editor.
2. (Facultatif) Choisissez le Régions AWS domaine dans lequel vous souhaitez rechercher les ressources à étiqueter. Par défaut, votre région actuelle est utilisée. Pour cette procédure, choisissez us-east-1 et us-west-2.
3. Choisissez au moins un type de ressource dans la liste déroulante des types de ressources. Vous pouvez ajouter ou modifier des balises pour un maximum de 20 types de ressources individuelles à la fois, ou choisir All resource types (Tous les types de ressources). Pour cette procédure, sélectionnez AWS::EC2::Instanceet AWS::S3::Bucket.
4. (Facultatif) Dans les champs Balises, entrez une clé de balise, ou une paire clé-valeur de balise, pour limiter les ressources actuelles Région AWS à celles qui sont étiquetées avec les valeurs que vous avez spécifiées. Lorsque vous entrez une clé de balise, les clés de balise correspondantes dans la région actuelle apparaissent dans une liste. Vous pouvez choisir une clé de balise dans la liste. Tag Editor remplit automatiquement la clé de balise pour vous lorsque vous saisissez suffisamment de caractères correspondants à une clé existante. 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 la balise est facultative mais permet de restreindre davantage les résultats de la requête. Choisissez Add (Ajouter) pour ajouter plus de balises. Les requêtes attribuent un `AND` opérateur aux balises, de sorte que seules les ressources correspondant à la fois au type de ressource spécifié et à toutes les balises spécifiées sont renvoyées par la requête.

> **Note**
>
> La console Tag Editor ne prend actuellement pas en charge les caractères génériques.

Pour rechercher des ressources avec plusieurs valeurs pour une clé de balise, ajoutez une autre balise avec la même clé à la requête, mais spécifiez une valeur différente. Les résultats comprennent toutes les ressources qui sont balisées avec la même clé de balise et qui ont l'une des valeur sélectionnées. La recherche est sensible à la casse.

Laissez les champs Tags vides pour trouver toutes les ressources du type spécifié dans le champ sélectionné Régions AWS. Cette requête renvoie les ressources qui ont des balises, ainsi que celles qui n'ont pas de balises. Pour supprimer une balise de votre requête, choisissez X sur l'étiquette de la balise.

Pour rechercher les ressources dotées d'une balise, mais dont la valeur est vide, choisissez (valeur vide).

> **Note**
>
> Avant de pouvoir trouver des ressources avec les balises spécifiées, celles-ci doivent avoir été appliquées à au moins une ressource du type spécifié dans le fichier actuel Région AWS.

5. Lorsque votre requête est prête, cliquez sur Search resources (Rechercher des ressources). Les résultats sont affichés sous forme de tableau dans la zone des résultats de recherche de ressources.

   Pour filtrer un grand nombre de ressources, saisissez un filtre de texte, comme une partie du nom d'une ressource dans les Filter resources (Filtrer les ressources).

   > **Note**
   >
   > Vous pouvez utiliser des sous-chaînes pour filtrer les résultats.

6. (Facultatif) Pour configurer les colonnes que l'éditeur de balises affiche dans les résultats de recherche de ressources, cliquez sur l'icône en forme de roue de préférences dans les résultats de recherche de ressources.

Sur la page Preferences (Préférences), choisissez le nombre de lignes que vous souhaitez afficher dans vos résultats de recherche. Si vous souhaitez voir tout le texte du tableau, cochez la case Envelopper les lignes.

Activez les colonnes que vous voulez que Tag Editor affiche dans vos résultats. Vous pouvez afficher une colonne pour chaque balise figurant dans les résultats de recherche ou pour un sous-ensemble sélectionné de vos résultats de recherche. Vous pouvez le faire à tout moment une fois que vous avez trouvé des ressources à étiqueter. Pour activer une colonne, cliquez sur l'icône du commutateur à côté de la balise et remplacez-la par Activée.

Lorsque vous avez terminé la configuration des colonnes visibles et le nombre de lignes affichées, choisissez Confirm (Confirmer).

Afficher et modifier les balises existantes pour une ressource sélectionnée

L'éditeur de balises affiche les balises existantes sur les ressources sélectionnées qui figurent dans les résultats de votre requête Find resources to tag.

Si vous avez activé une colonne Tag comme décrit dans la section précédente, vous pouvez voir la valeur actuelle de cette balise pour chaque ressource dans les résultats de recherche.

> **Note**
>
> Cette rubrique explique comment modifier le tag d'une ressource individuelle. Vous pouvez également modifier en bloc les balises de plusieurs ressources sélectionnées en même temps. Pour de plus amples informations, veuillez consulter Gestion des balises avec l'éditeur de balises.

Pour modifier les balises en ligne dans le tableau des résultats de recherche

1. Choisissez la valeur de la balise de la ressource que vous souhaitez modifier.

> **Note**
>
> - Si la ressource choisie ne possède actuellement aucune balise avec la clé choisie, la valeur s'affiche sous la forme (non balisée).
> - Si la ressource choisie possède une étiquette avec la clé choisie mais sans valeur, la valeur s'affiche sous la forme « — ».

2. Vous pouvez saisir une nouvelle valeur ou choisir l'une des valeurs déjà présentes sur d'autres ressources avec cette balise. Vous pouvez également supprimer le tag de cette ressource en choisissant Supprimer le tag.

Pour afficher tous les tags d'une ressource individuelle

1. Dans les résultats de votre requête Rechercher des ressources à étiqueter, choisissez le numéro dans la colonne Tags pour toute ressource pour laquelle vous souhaitez afficher les balises existantes. Les ressources avec un tiret dans la colonne Tags (Balises) n'ont pas de balises existantes.
2. Affichage des balises existantes dans les Resource tags (Balises des ressource). Vous pouvez également ouvrir cette fenêtre en choisissant Gérer les balises des ressources sélectionnées, lorsque vous modifiez ou supprimez des balises sur la page Gérer les balises.

> **Note**
>
> Si vous ne voyez pas une balise que vous venez d'appliquer à une ressource, actualisez la fenêtre de votre navigateur.

Exporter les résultats vers un fichier .csv

Vous pouvez exporter les résultats d'une requête Find resources to tag vers un fichier de valeurs séparées par des virgules (.csv). Le fichier .csv inclut les noms des ressources, les services, la région, la ressource IDs, le nombre total de balises et une colonne pour chaque clé de balise unique de la collection. Le fichier .csv peut vous aider à développer une stratégie de balisage pour les ressources de votre organisation, ou à déterminer les chevauchements ou les incohérences dans le balisage des ressources.

1. Dans les résultats de votre requête Find resources to tag (Rechercher des ressources à baliser), choisissez Export resources to CSV (Exporter les ressources au format CSV).
2. Lorsque votre navigateur vous le demande, choisissez d'ouvrir le fichier .csv ou de l'enregistrer à un emplacement approprié.

Gestion des balises avec l'éditeur de balises

Une fois que vous avez trouvé les ressources que vous souhaitez baliser, vous pouvez ajouter, supprimer et modifier les balises de certains ou de tous vos résultats de recherche. L'éditeur de balises affiche toutes les balises associées aux ressources. Il indique également si ces balises ont été ajoutées dans l'éditeur de balises, par la console de service de la ressource ou à l'aide de l'API.

Important

Ne stockez pas d'informations personnelles 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.

Autres moyens de gérer vos tags

Cette rubrique décrit le balisage des ressources à l'aide de l'éditeur de balises dans le Console de gestion AWS. Toutefois, vous pouvez également gérer les balises de vos AWS ressources à l'aide des outils suivants :

- Vous pouvez taper ou écrire des commandes à l'invite de votre interpréteur de `resourcegroupstaggingapi`commandes en utilisant les commandes du AWS Command Line Interface (AWS CLI).
- Vous pouvez créer et exécuter des PowerShell scripts à l'aide de l'API de Groupes de ressources AWS balisage dans le AWS Tools for PowerShell Core.
- Vous pouvez créer et exécuter des programmes avec n'importe lequel des éléments disponibles en AWS SDKsutilisant le balisage des groupes de ressources APIs, tel que le balisage pour APIs Python ou le balisage APIs pour Java.

Lorsque vous ajoutez, supprimez ou modifiez des balises existantes, vous modifiez les balises uniquement pour les ressources que vous sélectionnez dans les résultats de votre requête Rechercher des ressources à étiqueter. Vous pouvez sélectionner jusqu'à 500 ressources sur lesquelles gérer les balises.

Ajouter des balises aux ressources sélectionnées

Vous pouvez utiliser Tag Editor pour ajouter des balises aux ressources sélectionnés qui se trouvent dans les résultats de votre requête. Find resources to tag (Rechercher des ressources à baliser).

> **Note**
>
> Cette rubrique explique comment modifier en bloc les balises de plusieurs ressources. Vous pouvez également modifier les valeurs des balises pour une ressource individuelle. Pour de plus amples informations, veuillez consulter Afficher et modifier les balises existantes pour une ressource sélectionnée.

1. Ouvrez la console Tag Editor et soumettez une requête qui renvoie plusieurs ressources que vous souhaitez baliser.
2. Dans le tableau des résultats de votre requête Rechercher des ressources à étiqueter, cochez les cases à côté des ressources auxquelles vous souhaitez ajouter des balises. Entrez une chaîne de texte dans Filtrer les ressources en haut du tableau pour filtrer une partie du nom, de l'ID, des clés de balise ou des valeurs de balise d'une ressource. Dans la colonne Tags (Balises), notez que des balises sont déjà appliquées aux ressources dans les résultats.
3. Cochez la case correspondant à une ou plusieurs ressources, puis choisissez Gérer les balises des ressources sélectionnées.
4. Sur la page Manage tas (Gérer les balises), afficher les balises sur les ressources que vous avez sélectionnées. Bien que votre requête initiale ait renvoyé davantage de ressources, vous ajoutez des balises uniquement aux ressources que vous avez sélectionnées à l'étape 1. Choisissez Ajouter une balise.
5. Saisissez une clé de balise et une valeur de balise facultative. Pour cette procédure, vous allez ajouter la clé de balise **`Team`** et la valeur de la balise**`Development`**.

   > **Note**
   >
   > Une ressource peut compter un maximum de 50 balises appliquées par l'utilisateur. Il se peut que vous ne puissiez pas ajouter de nouvelles balises à une ressource si vous approchez les 50 balises appliquées par l'utilisateur. AWS les balises générées ne s'appliquent pas à la limite de 50 balises. Les clés de balises doivent également être uniques dans vos ressources sélectionnées. Vous ne pouvez pas ajouter une nouvelle

balise dont la clé correspond à une clé de balise qui existe déjà dans les ressources que vous avez sélectionnées.

6. Lorsque vous avez terminé d'ajouter des balises, choisissez Vérifier et appliquer les modifications.
7. Si vous acceptez les modifications, choisissez Apply changes to all selected (Appliquer les modifications à toute la sélection).
8. Selon le nombre de ressources que vous sélectionnez, l'application de nouvelles balises peut prendre quelques minutes. Ne quittez pas la page et n'ouvrez pas une autre page dans le même onglet du navigateur. Si des modifications ont été réalisées avec succès, une bannière verte de succès s'affiche en haut de la page. Attendez qu'une bannière de succès ou d'échec bannière s'affiche sur la page avant de continuer.

   Si les modifications de balises apportées à certaines ou à toutes les ressources n'aboutissent pas, consultez la section Résolution des problèmes liés aux modifications de balises. Après avoir résolu les modifications de balises infructueuses (telles que des autorisations insuffisantes), vous pouvez réessayer de modifier les balises sur les ressources pour lesquelles les modifications de balises ont échoué. Pour de plus amples informations, veuillez consulter the section called "Réessayer les modifications de balises qui ont échoué".

Modifier les balises des ressources sélectionnées

Vous pouvez utiliser Tag Editor pour modifier les valeurs de balises existantes sur des ressources sélectionnées qui se trouvent dans les résultats de votre requête Find resources to tag (Rechercher des ressources à baliser). La modification d'une balise change sa valeur pour toutes les ressources sélectionnées qui ont la même clé de balise. Vous ne pouvez pas renommer une clé de balise, mais vous pouvez supprimer une balise et créer une balise avec un nouveau nom pour remplacer la clé de balise d'origine. Cela supprime toutes les balises avec cette clé pour les ressources sélectionnées.

⚠ Important

Ne stockez pas d'informations personnelles 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.

1. Dans les résultats de votre requête Find resources to tag (Rechercher des ressources à baliser), cochez les cases en regard des ressources pour lesquelles vous souhaitez modifier les balises existantes. Saisissez une chaîne de texte dansFilter resources (Filtre les resources) pour filtrer une partie d'un nom ou ID d’une ressource Dans la colonne Tags (Balises), notez que des balises sont déjà appliquées aux ressources dans les résultats.
2. Choisissez Manage tags of the selected resources (Gérer les balises des ressources sélectionnées).
3. Sur la page Manage tags (Gérer les balises), dans Edit tags of selected resources (Modifier les balises des ressources sélectionnées), consultez les balises pour la ressource que vous avez sélectionnée. Bien que votre requête initiale ait renvoyé davantage de ressources, vous modifiez les balises uniquement pour les ressources que vous avez sélectionnées à l'étape 1.
4. Modifiez, ajouter ou supprimer des valeurs de balise. Les balises existantes doivent avoir une clé de balise, mais les valeurs de balise sont facultatives.

   Dans cette procédure, nous changeons la valeur de la **`Team`** balise en**`QA`**.

   Si les ressources de votre sélection ont des valeurs différentes pour la même clé, les ressources sélectionnées ont des valeurs de balise différentes s'affiche dans le champ Valeur de balise. Dans ce cas, le fait de placer votre curseur dans la case ouvre une liste déroulante de toutes les valeurs disponibles pour cette clé de balise dans les ressources que vous avez sélectionnées.

   Si les ressources de votre sélection ont la valeur de balise que vous voulez, la valeur de balise est mise en surbrillance pendant que vous la saisissez. Par exemple, si les ressources de votre sélection ont déjà la valeur de balise **`QA`**, elle est mise en surbrillance pendant que vous saisissez **`Q`**. Les valeurs de la liste déroulante permettent de maintenir la cohérence des valeurs des balises dans toutes les ressources. La valeur de balise est modifiée pour toutes les ressources sélectionnées. Dans cet exemple, la valeur de balise est remplacée par **`QA`** pour toutes les ressources sélectionnées ayant eu une clé de balise **`Team`**. Pour les ressources sélectionnées qui ne possèdent pas le **`Team`** tag, le **`Team`** tag avec la valeur **`QA`** est ajouté.
5. Lorsque vous avez terminé de modifier les balises, choisissez Vérifier et appliquer les modifications.
6. Si vous acceptez les modifications, choisissez Apply changes to all selected (Appliquer les modifications à toute la sélection).
7. En fonction du nombre de ressources que vous avez sélectionnées, la modification de balises peut prendre quelques minutes. Ne quittez pas la page et n'ouvrez pas une autre page dans le même onglet du navigateur. Si des modifications ont été réalisées avec succès, une bannière

verte de succès s'affiche en haut de la page. Attendez qu'une bannière de succès ou d'échec bannière s'affiche sur la page avant de continuer.

Si les modifications de balises apportées à certaines ou à toutes les ressources n'aboutissent pas, consultez la section Résolution des problèmes liés aux modifications de balises. Une fois que vous avez résolu les causes principales de l'échec des modifications de balises (telles que des autorisations insuffisantes), vous pouvez réessayer de modifier les balises sur les ressources pour lesquelles les modifications de balises ont échoué. Pour de plus amples informations, veuillez consulter the section called "Réessayer les modifications de balises qui ont échoué".

Supprimer les balises des ressources sélectionnées

Vous pouvez utiliser Tag Editor pour supprimer des balises des ressources sélectionnées qui se trouvent dans les résultats de votre requête Find resources to tag (Rechercher des ressources à baliser). La suppression d'une balise élimine la balise de toutes les ressources sélectionnées qui ont la balise. Comme vous ne pouvez pas modifier les clés de balise, vous pouvez supprimer des balises et les remplacer par de nouvelles balises si vous devez modifier une clé de balise. Cela supprime toutes les balises avec cette clé pour les ressources sélectionnées.

1. Dans les résultats de votre requête Find resources to tag (Rechercher des ressources à baliser), cochez les cases en regard des ressources pour lesquelles vous souhaitez supprimer des balises. Saisissez une chaîne de texte dansFilter resources (Filtre les resources) pour filtrer une partie d'un nom ou ID d'une ressource
2. Choisissez Manage tags of the selected resources (Gérer les balises des ressources sélectionnées).
3. Sur la page Manage tags (Gérer les balises), dans Edit tags of selected resources (Modifier les balises des ressources sélectionnées), consultez les balises pour les ressources que vous avez sélectionnées. Bien que votre requête initiale ait renvoyé davantage de ressources, vous modifiez les balises uniquement pour les ressources que vous avez sélectionnées à l'étape 1.
4. Choisissez Remove tag (Supprimer une balise) en regard de toutes les balises que vous souhaitez supprimer. Dans cette procédure, nous retirons le **`Team`** tag.

> **Note**
>
> En choisissant Remove tag (Supprimer la balise), nous supprimons une balise de toutes les ressources sélectionnées qui ont la balise.

5. Choisissez Review and apply changes (Vérifier et appliquer les modifications).
6. Sur la page de confirmation, choisissez Apply changes to all selected (Appliquer les modifications à toute la sélection).
7. En fonction du nombre de ressources que vous avez sélectionnées, la suppression des balises peut prendre quelques minutes. Ne quittez pas la page et n'ouvrez pas une autre page dans le même onglet du navigateur. Si des modifications ont été réalisées avec succès, une bannière verte de succès s'affiche en haut de la page. Attendez qu'une bannière de succès ou d'échec bannière s'affiche sur la page avant de continuer.

   Si des modifications de balises pour certaines ou toutes les ressources ont échoué, consultez Dépannage de la modification des balises. Une fois que vous avez résolu les causes principales de l'échec des modifications de balises (telles que des autorisations insuffisantes), vous pouvez réessayer de modifier les balises sur les ressources pour lesquelles les modifications de balises ont échoué. Pour de plus amples informations, veuillez consulter the section called "Réessayer les modifications de balises qui ont échoué".

Utilisation de balises dans les politiques d'autorisation IAM

Gestion des identités et des accès AWS (IAM) est celui Service AWS que vous utilisez pour créer et gérer des politiques d'autorisation qui déterminent qui peut accéder à vos AWS ressources. Chaque tentative d'accès à un AWS service ou de lecture ou d'écriture d'une AWS ressource est contrôlée par une politique IAM.

Ces politiques vous permettent de fournir un accès granulaire à vos ressources. L'une des fonctionnalités que vous pouvez utiliser pour affiner cet accès est l'`Condition`élément de la politique. Cet élément vous permet de spécifier les conditions qui doivent correspondre à la demande afin de déterminer si celle-ci peut être traitée. Parmi les éléments que vous pouvez vérifier avec l'`Condition`élément, citons les suivants :

- Balises associées à l'utilisateur ou au rôle à l'origine de la demande.
- Balises associées à la ressource faisant l'objet de la demande.

Contrôle d'accès basé sur les balises et les attributs

Les tags peuvent jouer un rôle important dans votre stratégie de contrôle AWS d'accès. Pour plus d'informations sur l'utilisation des balises comme attributs dans une stratégie de contrôle d'accès basé sur les attributs (ABAC), voir Contrôle de l'accès aux AWS ressources à l'aide de balises et Contrôle de l'accès aux utilisateurs et aux rôles IAM à l'aide de balises, tous deux dans le Guide de l'utilisateur IAM.

Il existe un didacticiel complet qui explique comment accorder l'accès à différents projets et groupes à l'aide de balises dans le didacticiel IAM : Définissez les autorisations d'accès aux AWS ressources en fonction des balises du guide de l'Gestion des identités et des accès AWS utilisateur.

Si vous utilisez un fournisseur d'identité (IdP) basé sur le protocole SAML pour l'authentification unique, vous pouvez associer des balises aux rôles assumés fournissant un accès à vos utilisateurs. Pour plus d'informations, consultez le didacticiel IAM : Utiliser les balises de session SAML pour ABAC dans le guide de l'Gestion des identités et des accès AWS utilisateur.

Clés de condition liées aux balises

Le tableau suivant décrit les clés de condition que vous pouvez utiliser dans une politique d'autorisation IAM pour contrôler l'accès en fonction des balises. Ces clés de condition vous permettent d'effectuer les opérations suivantes :

- Comparez les balises du principal appelant l'opération.
- Comparez les balises fournies à l'opération en tant que paramètre.
- Comparez les balises associées à la ressource à laquelle l'opération doit accéder.

Pour plus de détails sur une clé de condition et sur son utilisation, consultez la page liée dans la colonne Nom de la clé de condition.

Nom de la clé de condition	Description
aws:PrincipalTag	Compare le tag attaché au principal (rôle ou utilisateur IAM) qui fait la demande avec le tag que vous spécifiez dans la politique.
aws:RequestTag	Compare la paire clé-valeur de balise transmise à la demande en tant que paramètre avec la paire clé-valeur de balise que vous spécifiez dans la politique.
aws:ResourceTag	Compare la paire clé-valeur attachée à la ressource avec la paire clé-valeur de balise que vous spécifiez dans la politique.
aws:TagKeys	Compare uniquement les clés de balise de la demande avec les clés que vous spécifiez dans la politique.

Exemples de politiques IAM utilisant des balises

Example Exemple 1 : Forcer les utilisateurs à attacher une balise spécifique lorsqu'ils créent une ressource

L'exemple de politique d'autorisation IAM suivant montre comment obliger l'utilisateur qui crée ou modifie les balises d'une politique IAM à inclure une balise avec la clé. `0wner` En outre, la politique exige que la valeur de la balise soit définie sur la même valeur que celle de la `0wner` balise

actuellement attachée au principal appelant. Pour que cette stratégie fonctionne, un `Owner` tag doit être attaché à tous les principaux, et les utilisateurs doivent être empêchés de modifier ce tag. Si une tentative de création ou de modification d'une politique a lieu sans inclure la `Owner` balise, la politique ne correspond pas et l'opération n'est pas autorisée.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/
Owner}"}
            }
        }
    ]
}
```

Example Exemple 2 : utiliser des balises pour limiter l'accès à une ressource à son « propriétaire »

L'exemple suivant de politique d'autorisation IAM permet à l'utilisateur d'arrêter une instance Amazon EC2 en cours d'exécution uniquement si le principal appelant est étiqueté avec la `project` même valeur de balise que l'instance.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
      }
    }
  ]
}
```

Cet exemple est un exemple de contrôle d'accès basé sur les attributs (ABAC). Pour plus d'informations et d'autres exemples d'utilisation des politiques IAM pour mettre en œuvre une stratégie de contrôle d'accès basée sur des balises, consultez les rubriques suivantes du guide de l'Gestion des identités et des accès AWS utilisateur :

- Contrôle de l'accès aux AWS ressources à l'aide de balises
- Contrôle de l'accès aux utilisateurs et aux rôles IAM et pour ceux-ci à l'aide de balises
- Tutoriel IAM : définissez les autorisations d'accès aux AWS ressources en fonction des balises — Montre comment accorder l'accès à différents projets et groupes à l'aide de plusieurs balises.

AWS Organizations politiques relatives aux balises

Une politique de balises est un type de politique que vous créez dans AWS Organizations. Vous pouvez utiliser les politiques relatives aux balises pour normaliser les balises entre les ressources des comptes de votre organisation. Pour utiliser les politiques de balises, nous vous recommandons de suivre les flux de travail décrits dans la section Commencer à utiliser les politiques de balises du Guide de AWS Organizations l'utilisateur. Comme indiqué sur cette page, les flux de travail recommandés incluent la recherche et la correction des balises non conformes. Pour effectuer ces tâches, vous devez utiliser la console Tag Editor.

Conditions préalables et autorisations

Avant de pouvoir évaluer la conformité aux politiques de balises dans l'éditeur de balises, vous devez satisfaire aux exigences et définir les autorisations nécessaires.

Rubriques

- Conditions préalables à l'évaluation de la conformité aux politiques relatives aux balises
- Autorisations pour évaluer la conformité d'un compte
- Autorisations pour évaluer la conformité à l'échelle de l'organisation
- Politique relative aux compartiments Amazon S3 pour le stockage des rapports

Conditions préalables à l'évaluation de la conformité aux politiques relatives aux balises

L'évaluation de la conformité aux politiques relatives aux balises nécessite les éléments suivants :

- Vous devez d'abord activer la fonctionnalité dans AWS Organizations, puis créer et joindre des politiques de balises. Pour plus d'informations, consultez les pages suivantes du guide de l'AWS Organizations utilisateur :
  - Conditions préalables et autorisations pour gérer les politiques relatives aux balises
  - Activation des politiques relatives aux balises
  - Commencer à utiliser les politiques relatives aux balises
- Pour détecter des balises non conformes sur les ressources d'un compte, vous avez besoin des informations de connexion associées à ce compte et des autorisations répertoriées dans. Autorisations pour évaluer la conformité d'un compte

- Pour évaluer la conformité à l'échelle de l'organisation, vous avez besoin d'informations d'identification pour le compte de gestion de l'organisation et des autorisations répertoriées dans. Autorisations pour évaluer la conformité à l'échelle de l'organisation Vous ne pouvez demander le rapport de conformité qu'à l'est des Région AWS États-Unis (Virginie du Nord).

Autorisations pour évaluer la conformité d'un compte

La détection de balises non conformes sur les ressources d'un compte nécessite les autorisations suivantes :

- `organizations:DescribeEffectivePolicy`— Pour obtenir le contenu de la politique de balises en vigueur pour le compte.
- `tag:GetResources`— Pour obtenir une liste des ressources qui ne sont pas conformes à la politique en matière de balises ci-jointe.
- `tag:TagResources`— Pour ajouter ou mettre à jour des balises. Vous avez également besoin d'autorisations spécifiques au service pour créer des balises. Par exemple, pour baliser des ressources dans Amazon Elastic Compute Cloud (Amazon EC2), vous avez besoin d'autorisations pour. `ec2:CreateTags`
- `tag:UnTagResources`— Pour supprimer un tag. Vous devez également disposer d'autorisations spécifiques au service pour supprimer des balises. Par exemple, pour débaliser des ressources dans Amazon EC2, vous avez besoin d'autorisations pour. `ec2:DeleteTags`

L'exemple de politique Gestion des identités et des accès AWS (IAM) suivant fournit des autorisations pour évaluer la conformité des balises d'un compte.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
```

```
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur les politiques et les autorisations IAM, consultez le Guide de l'utilisateur IAM.

Autorisations pour évaluer la conformité à l'échelle de l'organisation

L'évaluation de la conformité à l'échelle de l'organisation avec les politiques relatives aux balises nécessite les autorisations suivantes :

- `organizations:DescribeEffectivePolicy`— Pour obtenir le contenu de la politique de balises attachée à l'organisation, à l'unité organisationnelle (UO) ou au compte.
- `tag:GetComplianceSummary`— Pour obtenir un résumé des ressources non conformes dans tous les comptes de l'organisation.
- `tag:StartReportCreation`— Exporter les résultats de l'évaluation de conformité la plus récente vers un fichier. Organization-wide la conformité est évaluée toutes les 48 heures.
- `tag:DescribeReportCreation`— Pour vérifier l'état de la création du rapport.
- `s3:ListAllMyBuckets`— Pour faciliter l'accès au rapport de conformité à l'échelle de l'organisation.
- `s3:GetBucketAcl`— Pour inspecter la liste de contrôle d'accès (ACL) du compartiment Amazon S3 recevant le rapport de conformité.
- `s3:GetObject`— Pour récupérer le rapport de conformité depuis le compartiment Amazon S3 appartenant au service.
- `s3:PutObject`— Pour placer le rapport de conformité dans le compartiment Amazon S3 spécifié.
- `s3:PutObject`avec `Null: {s3:x-amz-copy-source: true}` — Nécessaire pour autoriser les opérations de téléchargement partitionné (`InitiateMultipartUpload`,`CompleteMultipartUpload`) lorsque le service fournit des rapports de conformité volumineux. Ces opérations n'incluent pas d'en-tête de source de copie, elles nécessitent donc une déclaration distincte de celle de la livraison basée sur la copie.

Si le compartiment Amazon S3 dans lequel le rapport est envoyé est chiffré SSE-KMS, vous devez également disposer de l'`kms:GenerateDataKey`autorisation pour ce compartiment.

L'exemple de politique IAM suivant fournit des autorisations pour évaluer la conformité à l'échelle de l'organisation. Remplacez chacune *`placeholder`* par vos propres informations :

- *`bucket_name`*— Le nom de votre compartiment Amazon S3
- *`organization_id`*— L'identifiant de votre organisation

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
```

```
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/
*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
            }
        },
        {
            "Sid": "PutObjectCreateMultipartUpload",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/
*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "Null": {
                    "s3:x-amz-copy-source": "true"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur les politiques et les autorisations IAM, consultez le Guide de l'utilisateur IAM.

Politique relative aux compartiments Amazon S3 pour le stockage des rapports

Pour créer un rapport de conformité à l'échelle de l'organisation, l'identité que vous utilisez pour appeler l'`StartReportCreation`API doit avoir accès à un bucket Amazon Simple Storage Service (Amazon S3) dans la région USA Est (Virginie du Nord) pour stocker le rapport. Tag Policies utilise les informations d'identification de l'identité appelante pour transmettre le rapport de conformité au compartiment spécifié.

Si le compartiment et l'identité utilisés pour appeler l'`StartReportCreation`API appartiennent au même compte, des politiques de compartiment Amazon S3 supplémentaires ne sont pas nécessaires pour ce cas d'utilisation.

Si le compte associé à l'identité utilisée pour appeler l'`StartReportCreation`API est différent du compte propriétaire du compartiment Amazon S3, la politique de compartiment suivante doit être attachée au compartiment. Remplacez chacune *`placeholder`* par vos propres informations :

- *`bucket_name`*— Le nom de votre compartiment Amazon S3
- *`organization_id`*— L'identifiant de votre organisation
- *`identity_ARN`*— L'ARN de l'identité IAM utilisée pour appeler l'API `StartReportCreation`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
         },
         {
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/
*"
        }
    ]
}
```

Évaluation de la conformité d'un compte

Vous pouvez évaluer la conformité d'un compte de votre organisation à sa politique en matière de balises en vigueur.

> **Important**
>
> Les ressources non balisées n'apparaissent pas dans les résultats comme étant non conformes.
> Pour rechercher des ressources non balisées dans votre compte, utilisez-les AWS Resource Explorer avec une requête qui utilise**`tag:none`**. Pour plus d'informations, consultez la section Rechercher des ressources non balisées dans le guide de l'AWS Resource Explorer utilisateur.

La politique de balisage effective définit les règles de balisage qui s'appliquent à un compte. La politique de balise efficace est l'agrégation de toutes les politiques de balises dont le compte hérite, ainsi que de toutes les politiques de balises directement associées au compte. Lorsque vous attachez une politique de balises à la racine de l'organisation, elle s'applique à tous les comptes de votre organisation. Lorsque vous associez une politique de balises à une unité organisationnelle (UO), elle s'applique à tous OUs les comptes appartenant à l'UO.

> **Note**
>
> Si vous n'avez pas encore créé de politiques relatives aux balises, consultez la section Commencer à utiliser les politiques relatives aux balises dans le Guide de AWS Organizations l'utilisateur.

Pour rechercher des balises non conformes, vous devez disposer des autorisations suivantes :

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

Pour évaluer la conformité d'un compte à sa politique en matière de balises en vigueur (console)

1. Lorsque vous êtes connecté au compte dont vous souhaitez vérifier la conformité, ouvrez la console Tag Policies.
2. La section Politique de balise effective indique la date de dernière mise à jour de la politique et les clés de balise définies. Vous pouvez développer une clé de balise pour obtenir des informations sur ses valeurs, le traitement des cas et savoir si les valeurs sont appliquées à des types de ressources spécifiques.

   > **Note**
   >
   > Si vous êtes connecté au compte de gestion, vous devez choisir un compte pour connaître sa politique en vigueur et consulter les informations de conformité.

3. Dans la section Ressources contenant des balises non conformes, spécifiez les balises Région AWS à rechercher. Facultativement, vous pouvez également effectuer une recherche par type de ressource. Choisissez ensuite Rechercher des ressources.

   Les résultats en temps réel sont affichés dans la section Résultats de recherche. Pour modifier le nombre de résultats renvoyés par page ou les colonnes à afficher, cliquez sur l'icône des paramètres.
4. Dans les résultats de recherche, sélectionnez une ressource dont les balises ne sont pas conformes.
5. Dans la boîte de dialogue qui répertorie les balises de la ressource, cliquez sur le lien hypertexte pour ouvrir l' Service AWS endroit où la ressource a été créée. À partir de cette console, corrigez la balise non conforme.

> **Tip**
>
> Si vous ne savez pas quelles balises ne sont pas conformes, consultez la section Politique en matière de balises effective pour le compte dans la console Tag Policies. Vous pouvez développer une clé de balise pour afficher ses règles de balisage.

6. Répétez le processus de recherche et de correction des balises jusqu'à ce que les ressources du compte qui vous intéressent soient conformes dans chaque région.

Pour rechercher des balises non conformes (AWS CLI, AWS API)

Utilisez les commandes et opérations suivantes pour rechercher les balises non conformes :

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources
  - aws resourcegroupstaggingapi untag-resources

  Pour connaître la procédure complète d'utilisation des politiques de balises dans le AWS CLI, voir Utilisation des politiques de balises AWS CLI dans le Guide de AWS Organizations l'utilisateur.
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Étapes suivantes

Nous vous recommandons de répéter le processus de détection et de correction des problèmes de conformité. Continuez jusqu'à ce que les ressources du compte qui vous intéressent soient conformes à la politique de tag en vigueur dans chaque région.

La recherche et la correction de balises non conformes constituent un processus itératif pour plusieurs raisons, notamment les suivantes :

- L'utilisation des politiques relatives aux balises par votre organisation peut évoluer au fil du temps.

- Il faut du temps pour apporter des changements dans votre organisation lors de la création de ressources.
- La conformité peut changer à chaque fois qu'une nouvelle ressource est créée ou lorsque de nouvelles balises sont attribuées à une ressource.
- La politique de tag effective d'un compte est mise à jour chaque fois qu'une politique de tag y est attachée ou détachée. La politique de balises effective est également mise à jour chaque fois que des modifications sont apportées pour étiqueter les politiques dont le compte hérite.

Si vous êtes connecté en tant que compte de gestion dans l'organisation, vous pouvez également générer un rapport. Ce rapport contient des informations sur toutes les ressources étiquetées dans les comptes de votre organisation. Pour de plus amples informations, veuillez consulter Évaluation de la conformité à l'échelle de l'entreprise.

Évaluation de la conformité à l'échelle de l'entreprise

Vous pouvez évaluer la conformité de votre organisation à sa politique en matière de balises en vigueur. Vous pouvez générer un rapport répertoriant toutes les ressources étiquetées dans les comptes de votre organisation et indiquant si chaque ressource est conforme à la politique de balises en vigueur.

> **Important**
>
> Les ressources non balisées n'apparaissent pas dans les résultats comme étant non conformes.
> Pour rechercher des ressources non balisées dans votre compte, utilisez-les AWS Resource Explorer avec une requête qui utilise**`tag:none`**. Pour plus d'informations, consultez la section Rechercher des ressources non balisées dans le guide de l'AWS Resource Explorer utilisateur.

Vous pouvez générer le rapport `us-east-1` Région AWS uniquement à partir du compte de gestion de votre organisation. Le compte qui génère le rapport doit avoir accès à un compartiment Amazon S3 dans la région USA Est (Virginie du Nord). Le compartiment doit être associé à une politique de compartiment, comme indiqué dans le rapport sur la politique de compartiment d'Amazon S3 pour le stockage.

Pour générer un rapport de conformité à l'échelle de l'organisation, vous devez disposer des autorisations suivantes :

- `organizations:DescribeEffectivePolicy`
- `tag:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

Pour un exemple de politique IAM affichant ces autorisations, consultez Permissions pour évaluer la conformité à l'échelle de l'organisation.

Pour générer un rapport de conformité à l'échelle de l'organisation (console)

1. Ouvrez la console Tag Policies.
2. Choisissez l'onglet racine de cette organisation, puis en bas de la page, sélectionnez Générer un rapport.
3. Sur l'écran Générer un rapport, spécifiez où stocker le rapport.
4. Choisissez Commencer à exporter.

Lorsque le rapport est terminé, vous pouvez le télécharger depuis la section Rapport de non-conformité de l'onglet racine de l'organisation.

> **Remarques**
>
> La conformité à l'échelle de l'organisation est évaluée toutes les 48 heures. Il en résulte ce qui suit :
>
> - L'affichage des modifications apportées à une politique de balises ou à des ressources dans le rapport de conformité à l'échelle de l'organisation peut prendre jusqu'à 48 heures. Par exemple, supposons que vous disposez d'une politique de balises qui définit une nouvelle balise standardisée pour un type de ressources. Les ressources de ce type qui ne

possèdent pas cette balise peuvent apparaître comme conformes dans le rapport pendant 48 heures au maximum.

- Bien que vous puissiez générer le rapport à tout moment, les résultats du rapport ne sont pas mis à jour tant que la prochaine évaluation n'est pas terminée.
- La NoncompliantKeyscolonne répertorie les clés de balise de la ressource qui ne sont pas conformes à la politique de balise en vigueur.
- La KeysWithNonCompliantValuescolonne répertorie les clés définies dans la politique effective qui se trouvent sur la ressource avec un traitement de cas incorrect ou des valeurs non conformes.
- Si vous fermez une entreprise Compte AWS qui était membre de l'organisation, elle peut continuer à apparaître dans le rapport de conformité des balises pendant 90 jours au maximum.

Pour générer un rapport de conformité à l'échelle de l'organisation (AWS CLI, AWS API)

Utilisez les commandes et opérations suivantes pour générer un rapport de conformité à l'échelle de l'organisation, vérifier son statut et consulter le rapport :

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  Pour connaître la procédure complète d'utilisation des politiques de balises dans le AWS CLI, voir Utilisation des politiques de balises AWS CLI dans le Guide de AWS Organizations l'utilisateur.
- AWS API :
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

Surveillez les modifications des balises grâce aux flux de travail sans serveur et à Amazon EventBridge

Amazon EventBridge prend en charge les modifications de balises sur AWS les ressources. Ce EventBridge type vous permet de créer des EventBridge règles adaptées aux modifications de balises et d'acheminer les événements vers une ou plusieurs cibles. Par exemple, une cible peut être une AWS Lambda fonction permettant d'invoquer des flux de travail automatisés. Cette rubrique fournit un didacticiel sur l'utilisation de Lambda pour créer une solution sans serveur rentable afin de traiter en toute sécurité les modifications de balises sur vos ressources. AWS

Les modifications de balises génèrent des EventBridge événements

EventBridge fournit un flux d'événements système en temps quasi réel décrivant l'évolution des AWS ressources. De nombreuses AWS ressources prennent en charge les balises, qui sont des attributs personnalisés définis par l'utilisateur pour organiser et classer AWS facilement les ressources. Les exemples d'utilisation courants des balises sont la catégorisation de la répartition des coûts, la sécurité du contrôle d'accès et l'automatisation.

Avec EventBridge, vous pouvez surveiller les modifications apportées aux balises et suivre l'état des balises sur les AWS ressources. Auparavant, pour obtenir des fonctionnalités similaires, il se peut que vous ayez continuellement interrogé APIs et orchestré plusieurs appels. Désormais, toute modification apportée à une balise, y compris le service individuel APIs, l'éditeur de balises et l'API de balisage, initie le changement de balise lors de l'événement de ressource. L'exemple suivant montre un EventBridge événement typique provoqué par un changement de balise. Il affiche les clés de balise nouvelles, mises à jour ou supprimées, ainsi que leurs valeurs associées.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

Tous les EventBridge événements ont les mêmes champs de haut niveau :

- version — Par défaut, cette valeur est définie sur `0` (zéro) dans tous les événements.
- id — Une valeur unique est générée pour chaque événement. Cela peut être utile pour suivre les événements au fur et à mesure qu'ils passent des règles aux cibles et qu'ils sont traités.
- type de détail — Identifie, en combinaison avec le `source` champ, les champs et les valeurs qui apparaissent dans le champ de détail.
- source — Identifie le service à l'origine de l'événement. La source des modifications de balises est`aws.tag`.
- time — Horodatage de l'événement.
- région — Identifie l' Région AWS origine de l'événement.
- ressources — Ce tableau JSON contient les noms des ressources Amazon (ARNs) qui identifient les ressources impliquées dans l'événement. Il s'agit de la ressource où les balises ont été modifiées.
- detail — Objet JSON dont le contenu est différent selon le type d'événement. Pour le changement de balise sur une ressource, les champs détaillés suivants sont inclus :
  - changed-tag-keys— Les clés de balise modifiées par cet événement.
  - service — Le service auquel appartient la ressource. Dans cet exemple, le service est `ec2` Amazon EC2.

- resource-type — Type de ressource du service. Dans cet exemple, il s'agit d'une instance Amazon EC2.
- version — Version du jeu de balises. La version commence à 1 et augmente lorsque les balises sont modifiées. Vous pouvez utiliser la version pour vérifier l'ordre des événements de changement de balise.
- tags — Les balises associées à la ressource après la modification.

Pour plus d'informations, consultez les modèles EventBridge d'événements Amazon dans le guide de EventBridge l'utilisateur Amazon.

En utilisant EventBridge, vous pouvez créer des règles qui correspondent à des modèles d'événements spécifiques en fonction des différents champs. Nous expliquons comment procéder dans le didacticiel. Nous montrons également comment une instance Amazon EC2 peut être arrêtée automatiquement si aucune balise spécifiée n'est attachée à l'instance. Nous utilisons les EventBridge champs pour créer un modèle correspondant aux événements de balise pour l'instance qui lance une fonction Lambda.

Lambda et sans serveur

AWS Lambda suit le paradigme sans serveur pour exécuter du code dans le cloud. Vous n'exécutez du code que lorsque cela est nécessaire, sans penser aux serveurs. Vous ne payez que pour le temps de calcul exact que vous utilisez. Même s'il est appelé serverless, cela ne signifie pas qu'il n'y a pas de serveurs. Dans ce contexte, l'absence de serveur signifie que vous n'avez pas à approvisionner, configurer ou gérer les serveurs utilisés pour exécuter votre code. AWS fait tout cela pour vous, afin que vous puissiez vous concentrer sur votre code. Pour plus d'informations sur Lambda, consultez la présentation du AWS Lambda produit.

Tutoriel : arrêt automatique des instances Amazon EC2 auxquelles il manque les balises requises

À mesure que votre pool de AWS ressources et Comptes AWS que vous gérez augmente, vous pouvez utiliser des balises pour faciliter la catégorisation de vos ressources. Les balises sont couramment utilisées pour les cas d'utilisation critiques tels que la répartition des coûts et la sécurité. Pour gérer efficacement les AWS ressources, celles-ci doivent être systématiquement étiquetées. Souvent, lorsqu'une ressource est provisionnée, elle reçoit toutes les balises appropriées.

Cependant, un processus ultérieur peut entraîner une modification des balises qui déroge à la politique de l'entreprise en matière de balises. En surveillant les modifications apportées à vos balises, vous pouvez détecter leur dérive et réagir immédiatement. Cela vous donne davantage l'assurance que les processus qui dépendent de la bonne catégorisation de vos ressources produiront les résultats souhaités.

L'exemple suivant montre comment surveiller les modifications de balises sur les instances Amazon EC2 afin de vérifier qu'une instance spécifiée possède toujours les balises requises. Si les balises de l'instance changent et que l'instance ne possède plus les balises requises, une fonction Lambda est invoquée pour arrêter automatiquement l'instance. Pourquoi voudrais-tu faire ça ? Il garantit que toutes les ressources sont étiquetées conformément à la politique de votre entreprise en matière de balises, pour une allocation efficace des coûts ou pour pouvoir faire confiance à la sécurité basée sur le contrôle d'accès basé sur les attributs (ABAC).

Important

Nous vous recommandons vivement d'exécuter ce didacticiel dans un compte hors production où vous ne pouvez pas fermer par inadvertance des instances importantes. L'exemple de code présenté dans ce didacticiel limite intentionnellement l'impact de ce scénario aux seules instances d'une liste d'instances IDs. Vous devez mettre à jour la liste avec l'instance IDs que vous êtes prêt à arrêter pour le test. Cela permet de s'assurer que vous ne pouvez pas arrêter accidentellement toutes les instances d'une région de votre Compte AWS.

Après les tests, assurez-vous que toutes vos instances sont étiquetées conformément à la stratégie de balisage de votre entreprise. Vous pouvez ensuite supprimer le code qui limite la fonction à l'instance de IDs la liste uniquement.

Cet exemple utilise JavaScript et la version 16.x de. Node.js L'exemple utilise l' Compte AWS ID 123456789012 et le Région AWS US East (Virginie du Nord) (). `us-east-1` Remplacez-les par votre propre identifiant de compte test et votre propre région.

Note

Si votre console utilise une région différente par défaut, assurez-vous de changer de région dans ce didacticiel chaque fois que vous changez de console. L'échec de ce didacticiel est souvent dû au fait que l'instance et la fonction se trouvent dans deux régions différentes.

Si vous utilisez une région différente de la régionus-east-1, assurez-vous de remplacer toutes les références dans les exemples de code suivants par la région que vous avez choisie.

Rubriques

- Étape 1. Créer la fonction Lambda
- Étape 2. Configurer les autorisations IAM requises
- Étape 3. Effectuez un test préliminaire de votre fonction Lambda
- Étape 4 : Créez la EventBridge règle qui lance la fonction
- Étape 5. Testez la solution complète
- Résumé du didacticiel

Étape 1. Créer la fonction Lambda

Pour créer la fonction Lambda

1. Ouvrez la console AWS Lambda de gestion.
2. Choisissez Créer une fonction, puis sélectionnez Auteur à partir de zéro.
3. Pour Nom de la fonction, entrez **`AutoEC2Termination`**.
4. Pour Exécution, choisissez Node.js 16.x.
5. Conservez les valeurs par défaut de tous les autres champs, puis choisissez Create function.
6. Dans l'onglet Code de la page `AutoEC2Termination` détaillée, ouvrez le fichier index.js pour afficher son code.

   - Si un onglet contenant index.js est ouvert, vous pouvez sélectionner la zone d'édition de cet onglet pour modifier son code.
   - Si aucun onglet contenant index.js n'est ouvert, cliquez de nouveau sur le fichier index.js dans le dossier Auto EC2 Terminator dans le volet de navigation. Choisissez ensuite Open.
7. Dans l'onglet index.js, collez le code suivant dans la boîte de l'éditeur, en remplaçant tout ce qui est déjà présent.

   Remplacez la valeur `RegionToMonitor` par la région dans laquelle vous souhaitez exécuter cette fonction.

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match
```

```
const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
// safely stop

const InstanceList = [
    "i-0000000aaaaaaaaaa",
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
```

```
   return;
 }

 // If this event is not about an instance, then do nothing.
 if (!(resourceType === "instance")) {
   console.log("Event not for correct resource type -- no action (", resourceType,
")" );
   return;
 }

 // CAUTION - Removing the following 'if' statement causes the function to run
against
 //           every EC2 instance in the specified Region in the calling
Compte AWS.
 //           If you do this and an instance is not tagged with the approved tag
key
 //           and value, this function stops that instance.

 // If this event is not for the ARN of an instance in our include list, then do
nothing.
 if (InstanceList.indexOf(instanceId)<0) {
   console.log("Event not for one of the monitored instances -- no action (",
resource, ")");
   return;
 }

 console.log("Tags changed on monitored EC2 instance (",instanceId,")");

 // Check attached tags for expected tag key and value pair
 if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
   // Required tags ARE present
   console.log("The instance has the required tag key and value -- no action");
   callback(null, "no action");
   return;
 }

 // Required tags NOT present
 console.log("This instance is missing the required tag key or value -- attempting
to stop the instance");

 var params = {
   InstanceIds: [instanceId],
   DryRun: true
 };
```

```
  // call EC2 to stop the selected instances
  ec2.stopInstances(params, function(err, data) {
    if (err && err.code === 'DryRunOperation') {
      // dryrun succeeded, so proceed with "real" stop operation
      params.DryRun = false;
      ec2.stopInstances(params, function(err, data) {
        if (err) {
          console.log("Failed to stop instance");
          callback(err, "fail");
        } else if (data) {
          console.log("Successfully stopped instance", data.StoppingInstances);
          callback(null, "Success");
        }
      });
    } else {
      console.log("Dryrun attempt failed");
      callback(err);
    }
  });
};
```

8. Choisissez Déployer pour enregistrer vos modifications et activer la nouvelle version de la fonction.

Cette fonction Lambda vérifie les balises d'une instance Amazon EC2, comme indiqué par l'événement de changement de balise dans. EventBridge Dans cet exemple, s'il manque la clé de balise requise dans l'instance de l'événement `valid-key` ou si cette balise ne contient pas la valeur`valid-value`, la fonction essaie d'arrêter l'instance. Vous pouvez modifier cette vérification logique ou les exigences relatives aux balises pour vos propres cas d'utilisation spécifiques.

Gardez la fenêtre de la console Lambda ouverte dans votre navigateur.

Étape 2. Configurer les autorisations IAM requises

Avant que la fonction puisse s'exécuter correctement, vous devez lui accorder l'autorisation d'arrêter une instance EC2. Le rôle AWS fourni lambda_basic_executionne dispose pas de cette autorisation. Dans ce didacticiel, vous allez modifier la politique d'autorisation IAM par défaut attachée au rôle d'exécution de la fonction nomméAutoEC2Termination-role-*uniqueid*. L'autorisation supplémentaire minimale requise pour ce didacticiel est de`ec2:StopInstances`.

Pour plus d'informations sur la création de politiques IAM spécifiques à Amazon EC2, consultez Amazon EC2 : permet de démarrer ou d'arrêter une instance EC2 et de modifier un groupe de sécurité, par programmation et dans la console dans le guide de l'utilisateur IAM.

Pour créer une politique d'autorisation IAM et l'associer au rôle d'exécution de la fonction Lambda

1. Dans un autre onglet ou une autre fenêtre du navigateur, ouvrez la page Rôles de la console IAM.
2. Commencez à saisir le nom du rôle et**`AutoEC2Termination`**, lorsqu'il apparaît dans la liste, choisissez-le.
3. Sur la page Résumé du rôle, choisissez l'onglet Autorisations et choisissez le nom de la politique déjà attachée.
4. Sur la page Résumé de la politique, choisissez Modifier la politique.
5. Dans l'onglet Éditeur visuel, choisissez Ajouter des autorisations supplémentaires.
6. Pour Service, choisissez EC2.
7. Pour Actions, sélectionnez StopInstances. Vous pouvez saisir du **`Stop`** texte dans la barre de recherche, puis choisir le `StopInstances` moment où elle apparaît.
8. Pour Ressources, sélectionnez Toutes les ressources, sélectionnez Réviser la politique, puis sélectionnez Enregistrer les modifications.

   Cela crée automatiquement une nouvelle version de la politique et définit cette version comme version par défaut.

   Votre politique finale doit ressembler à l'exemple suivant.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
```

```
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/
lambda/AutoEC2Termination:*"
        }
    ]
}
```

Étape 3. Effectuez un test préliminaire de votre fonction Lambda

Au cours de cette étape, vous soumettez un événement de test à votre fonction. La fonctionnalité de test Lambda fonctionne en soumettant un événement de test fourni manuellement. La fonction traite l'événement de test comme s'il provenait de EventBridge. Vous pouvez définir plusieurs événements de test avec des valeurs différentes pour exercer toutes les différentes parties de votre code. Au cours de cette étape, vous soumettez un événement de test qui indique que les balises d'une instance Amazon EC2 ont changé et que les nouvelles balises n'incluent pas la clé et la valeur de balise requises.

Pour tester votre fonction Lambda

1. Retournez à la fenêtre ou à l'onglet avec la console Lambda et ouvrez l'onglet Test pour votre fonction de EC2 terminaison automatique.
2. Choisissez Créer un nouvel événement.
3. Dans Event name (Nom de l'événement), saisissez **`SampleBadTagChangeEvent`**.
4. Dans le JSON de l'événement, remplacez le texte par l'exemple d'événement illustré dans l'exemple de texte suivant. Il n'est pas nécessaire de modifier les comptes, la région ou l'ID d'instance pour que cet événement de test fonctionne correctement.

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

```
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3
  }
}
```

5. Choisissez Save (Enregistrer), puis Test (Tester).

   Le test semble échouer, mais ce n'est pas grave.

   L'erreur suivante devrait s'afficher dans l'onglet Résultats de l'exécution sous Réponse.

```
{
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
}
```

   L'erreur se produit parce que l'instance spécifiée dans l'événement de test n'existe pas.

   Les informations figurant dans l'onglet Résultats de l'exécution, dans la section Function Logs, montrent que votre fonction Lambda a tenté avec succès d'arrêter une instance EC2. Cependant, cela a échoué car le code tente initialement une DryRunopération pour arrêter l'instance, ce qui indique que l'ID d'instance n'était pas valide.

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
```

```
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. Pour prouver que le code n'essaie pas d'arrêter l'instance lorsque la bonne balise est utilisée, vous pouvez créer et soumettre un autre événement de test.

   Choisissez l'onglet Test au-dessus de la source du code. La console affiche votre événement de SampleBadTagChangeEventtest existant.

7. Choisissez Créer un nouvel événement.
8. Pour Nom de l'événement, tapez **`SampleGoodTagChangeEvent`**.
9. À la ligne 17, supprimez **`NOT-`** pour remplacer la valeur par**`valid-value`**.
10. En haut de la fenêtre de l'événement de test, choisissez Enregistrer, puis sélectionnez Test.

    La sortie affiche ce qui suit, qui montre que la fonction reconnaît la balise valide et ne tente pas d'arrêter l'instance.

```
START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
 instance has the required tag key and value -- no action
END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
```

Gardez la console Lambda ouverte dans votre navigateur.

Étape 4 : Créez la EventBridge règle qui lance la fonction

Vous pouvez désormais créer une EventBridge règle correspondant à l'événement et pointant vers votre fonction Lambda.

Pour créer la EventBridge règle

1. Dans un autre onglet ou une autre fenêtre du navigateur, ouvrez la EventBridge console sur la page Créer une règle.
2. Dans Nom, entrez**`ec2-instance-rule`**, puis choisissez Next.
3. Faites défiler l'écran jusqu'à Méthode de création et choisissez Modèle personnalisé (éditeur JSON).
4. Dans la zone d'édition, collez le texte du modèle suivant, puis choisissez Next.

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
```

```
}
```

Cette règle fait correspondre les `Tag Change on Resource` événements des instances Amazon EC2 et invoque ce que vous spécifiez comme cible à l'étape suivante.

5. Ajoutez ensuite votre fonction Lambda comme cible. Dans la zone Cible 1, sous Sélectionnez une cible, choisissez la fonction Lambda.
6. Sous Fonction, sélectionnez la fonction de EC2terminaison automatique que vous avez créée précédemment, puis cliquez sur Suivant.
7. Sur la page Configurer les balises, choisissez Next. Ensuite, sur la page Réviser et créer, choisissez Créer une règle. Cela autorise également automatiquement l'appel EventBridge de la fonction Lambda spécifiée.

Étape 5. Testez la solution complète

Vous pouvez tester votre résultat final en créant une instance EC2 et en observant ce qui se passe lorsque vous modifiez ses balises.

Pour tester la solution de surveillance avec une instance réelle

1. Ouvrez la console Amazon EC2 sur la page Instances.
2. Créez une instance Amazon EC2. Avant de le lancer, attachez une étiquette avec la clé `valid-key` et la valeur`valid-value`. Pour plus d'informations sur la création et le lancement d'une instance, consultez Étape 1 : Lancer une instance dans le guide de l'utilisateur Amazon EC2. Dans la procédure de lancement d'une instance, à l'étape 3, où vous entrez la balise Name, choisissez également Ajouter des balises supplémentaires, choisissez Ajouter une balise, puis entrez la clé **`valid-key`** et la valeur de**`valid-value`**. Vous pouvez continuer sans paire de clés si cette instance est uniquement destinée aux besoins de ce didacticiel et si vous prévoyez de supprimer cette instance une fois celle-ci terminée. Revenez à ce didacticiel à la fin de l'étape 1 ; vous n'avez pas besoin de suivre l'étape 2 : Se connecter à votre instance.
3. InstanceIdCopiez-le depuis la console.
4. Passez de la console Amazon EC2 à la console Lambda. Choisissez votre fonction de EC2terminaison automatique, cliquez sur l'onglet Code, puis sur l'onglet index.js pour modifier votre code.
5. Modifiez la deuxième entrée en `InstanceList` collant la valeur que vous avez copiée depuis la console Amazon EC2. Assurez-vous que la `RegionToMonitor` valeur correspond à la région qui contient l'instance que vous avez collée.

6. Choisissez Déployer pour activer vos modifications. La fonction est maintenant prête à être activée en modifiant les balises de cette instance dans la région spécifiée.
7. Passez de la console Lambda à la console Amazon EC2.
8. Modifiez les balises attachées à l'instance en supprimant la balise valid-key ou en modifiant la valeur de cette clé.

> **Note**
>
> Pour plus d'informations sur la façon de modifier les balises sur une instance Amazon EC2 en cours d'exécution, consultez la section Ajouter et supprimer des balises sur une ressource individuelle dans le guide de l'utilisateur Amazon EC2.

9. Patientez quelques secondes, puis actualisez la console. L'instance doit changer son état d'instance en Stopping, puis en Stopped.
10. Passez de la console Amazon EC2 à la console Lambda avec votre fonction, puis choisissez l'onglet Monitor.
11. Choisissez l'onglet Journaux, puis dans le tableau des appels récents, sélectionnez l'entrée la plus récente de la LogStreamcolonne.

    La CloudWatch console Amazon s'ouvre sur la page Log events pour le dernier appel de votre fonction Lambda. La dernière entrée doit ressembler à l'exemple suivant.

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

Résumé du didacticiel

Ce didacticiel explique comment créer une EventBridge règle correspondant à un changement de balise lors d'un événement de ressource pour les instances Amazon EC2. La règle pointait vers une fonction Lambda qui arrête automatiquement l'instance si elle ne possède pas la balise requise.

La EventBridge prise en charge par Amazon des modifications de balises sur les AWS ressources ouvre la voie à une automatisation axée sur les événements pour de nombreuses personnes. Services AWS La combinaison de cette fonctionnalité vous AWS Lambda fournit des outils pour créer des solutions sans serveur qui accèdent aux AWS ressources en toute sécurité, évoluent à la demande et sont rentables.

Les autres cas d'utilisation possibles de l' tag-change-on-resource EventBridge événement incluent :

- Lancez un avertissement si quelqu'un accède à votre ressource à partir d'une adresse IP inhabituelle : utilisez une balise pour enregistrer l'adresse IP source de chaque visiteur qui accède à votre ressource. Les modifications apportées à la balise génèrent un CloudWatch événement. Vous pouvez utiliser cet événement pour comparer l'adresse IP source à une liste d'adresses IP valides et activer un e-mail d'avertissement si l'adresse IP source n'est pas valide.
- Vérifiez si des modifications sont apportées à votre contrôle d'accès basé sur les balises pour une ressource : si vous avez configuré l'accès à une ressource à l'aide du contrôle d'accès basé sur les attributs (balises) (ABAC), vous pouvez utiliser les EventBridge événements générés par toute modification apportée à la balise pour demander à votre équipe de sécurité de procéder à un audit.

Résolution des problèmes de modification des balises

La liste de contrôle suivante peut être utile si des erreurs se produisent lorsque vous essayez d'appliquer ou modifier des balises sur les ressources sélectionnées dans Find resources to tag (Rechercher des ressources à baliser).

- La ressource pourrait déjà avoir le nombre maximal de balises. En général, les ressources peuvent avoir un maximum de 50 balises définies par l'utilisateur. AWS les balises générées ne sont pas prises en compte dans le calcul du maximum de 50 balises. D'autres utilisateurs peuvent également être en train d'ajouter des balises à la même ressource en même temps, ce qui peut faire atteindre le maximum de balises.
- Certains services autorisent un autre jeu de caractères (ou limitent le jeu de caractères qui est autorisé) pour créer des balises. Si vous avez ajouté ou modifié des balises contenant des caractères spéciaux, consultez les exigences relatives aux balises dans la documentation de service de la ressource pour vérifier que ces caractères sont autorisés par le service.
- Vous n'êtes peut-être pas autorisé à modifier les balises de la ressource. Si vous n'êtes pas autorisé à consulter les balises existantes d'une ressource, vous ne pouvez pas modifier les balises de la ressource.
- Vous n'êtes peut-être pas autorisé à modifier la ressource. Les modifications des métadonnées de la ressource peuvent être limitées par un autre administrateur.
- La ressource peut avoir été modifiée ou supprimée par un autre utilisateur ou processus. Supposons, par exemple, qu'une ressource ait été lancée dans le cadre de la création d'une CloudFormation pile. Si la pile a été supprimée ou n'est plus active, il est possible que la ressource ne soit plus disponible.
- Les balises ne peuvent peut-être plus être modifiées, si une ressource est hors ligne ou annulée, ou si d'autres mises à jour (par exemple, des mises à jour logicielles) sur la ressource sont en cours.
- Les modifications de balises peuvent échouer si vous fermez l'onglet du navigateur ou si vous modifiez la page avant que les modifications de balises ne soient terminées. Laisser les modifications des balises s'achever et attendez que la bannière de succès ou d'échec bannière apparaisse sur la page, avant de la quitter.
- Bien qu'il existe une limite de débit pour le AWS Resource Groups Tagging API, le service que vous balisez peut imposer une limite distincte que vous pourriez atteindre avant la limite de l'API Resource Groups Tagging.

Réessayer les modifications de balises qui ont échoué

Si les changements de balise échouent sur au moins l'une de vos ressources sélectionnées, Tag Editor affiche une bannière rouge en bas de la page. La bannière affiche un message d'erreur pour chaque type d'échec qui se produit. Pour chaque erreur, la bannière identifie les ressources spécifiques sur lesquelles l'éditeur de balises n'a pas pu modifier les balises. Après avoir examiné et résolu les erreurs, choisissez Réessayer les modifications de balises échouées sur les ressources pour réessayer les modifications uniquement sur les ressources pour lesquelles les modifications de balises ont échoué.

Sécurité dans l'éditeur de balises

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

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

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité. Pour plus d'informations sur les programmes de conformité qui s'appliquent à Tag Editor, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce 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 Tag Editor. Les rubriques suivantes expliquent comment configurer l'éditeur de balises pour répondre à vos objectifs de sécurité et de conformité.

Rubriques

- Protection des données dans Tag Editor
- Gestion des identités et des accès pour Tag Editor
- Journalisation et surveillance dans l'éditeur de balises
- Validation de conformité pour Tag Editor
- Résilience dans l'éditeur de balises
- Sécurité de l'infrastructure dans Tag Editor

Protection des données dans Tag Editor

Le modèle de responsabilité AWS partagée (modèle de) s'applique à la protection des données dans Tag Editor. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

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

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

Chiffrement des données

Les informations de balisage ne sont pas cryptées. Bien qu'elles ne soient pas chiffrées, les balises peuvent contenir des informations utilisées dans le cadre de votre stratégie de sécurité. Il est donc important de contrôler qui peut accéder aux balises sur les ressources. Il est particulièrement important de contrôler les personnes autorisées à modifier les balises, car un tel accès peut être utilisé pour augmenter les autorisations d'une personne.

Chiffrement au repos

Il n'existe aucun autre moyen spécifique à Tag Editor d'isoler le trafic de service ou de réseau. Le cas échéant, utilisez AWS un isolant spécifique. Vous pouvez utiliser l'API et la console Tag Editor dans un cloud privé virtuel (VPC) pour optimiser la confidentialité et la sécurité de l'infrastructure.

Chiffrement en transit

Les données de l'éditeur de balises 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

L'éditeur de balises n'est actuellement pas intégré AWS Key Management Service et n'est pas pris en charge AWS KMS keys.

Confidentialité du trafic inter-réseau

Tag Editor utilise le protocole HTTPS pour toutes les transmissions entre les utilisateurs de Tag Editor et AWS. L'éditeur de balises utilise le protocole TLS (Transport Layer Security) 1.3, mais prend également en charge le protocole TLS 1.2.

Gestion des identités et des accès pour Tag Editor

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources

de l'éditeur de balises. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment fonctionne Tag Editor avec IAM
- Exemples de politiques basées sur l'identité dans l'éditeur de balises
- Résolution des problèmes d'identité et d'accès à l'éditeur de balises

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès à l'éditeur de balises)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment fonctionne Tag Editor avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Exemples de politiques basées sur l'identité dans l'éditeur de balises)

Authentification par des identités

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

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Roles

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité

ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

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

Listes de contrôle d'accès (ACLs)

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

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, 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 des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

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

Comment fonctionne Tag Editor avec IAM

Avant d'utiliser IAM pour gérer l'accès à Tag Editor, vous devez connaître les fonctionnalités IAM disponibles avec Tag Editor. Pour obtenir une vue d'ensemble de la façon dont Tag Editor et d'autres outils Services AWS fonctionnent avec IAM, consultez Services AWS le guide de l'utilisateur d'IAM consacré à l'utilisation d'IAM.

Rubriques

- Politiques basées sur l'identité de l'éditeur de balises
- Politiques basées sur les ressources
- Autorisation basée sur les balises
- Rôles IAM de l'éditeur de balises

Politiques basées sur l'identité de l'éditeur de balises

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

Actions

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

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique dans Tag Editor utilisent le préfixe suivant avant l'action :`tag:`. Les actions de l'éditeur de balises sont entièrement exécutées dans la console, mais le préfixe figure `tag` dans les entrées du journal.

Par exemple, pour autoriser une personne à étiqueter une ressource avec l'opération d'`tag:TagResources`API, vous devez inclure l'`tag:TagResources`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. L'éditeur de balises

définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

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

```
"Action": [
      "tag:action1",
      "tag:action2",
      "tag:action3"
```

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

```
"Action": "tag:Get*"
```

Pour consulter la liste des actions de l'éditeur de balises, consultez la section Actions, ressources et clés de condition pour l'éditeur de balises dans la référence d'autorisation de service.

Ressources

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Tag Editor ne dispose d'aucune ressource propre. Il manipule plutôt les métadonnées (balises) associées aux ressources créées par d'autres Services AWS.

Clés de condition

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

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

L'éditeur de balises ne définit aucune clé de condition spécifique au service.

Exemples

Pour consulter des exemples de politiques basées sur l'identité de Tag Editor, consultez. Exemples de politiques basées sur l'identité dans l'éditeur de balises

Politiques basées sur les ressources

L'éditeur de balises ne prend pas en charge les politiques basées sur les ressources car il ne définit aucune de ses propres ressources.

Autorisation basée sur les balises

L'autorisation basée sur les balises fait partie de la stratégie de sécurité appelée contrôle d'accès basé sur les attributs (ABAC).

Pour contrôler l'accès à une ressource en fonction de ses balises, vous devez fournir des informations de balise dans l'élément de condition d'une politique à l'aide des clés `aws:ResourceTag/`*`key-name`*`aws:RequestTag/`*`key-name`*, ou de `aws:TagKeys` condition. Vous pouvez appliquer des balises à une ressource lors de sa création ou de sa mise à jour.

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 Afficher les groupes en fonction des balises. Pour plus d'informations sur le contrôle d'accès basé sur les attributs (ABAC), voir À quoi sert ABAC ? AWS dans le guide de l'utilisateur IAM.

Rôles IAM de l'éditeur de balises

Un rôle IAM est une entité au sein de vous Compte AWS qui possède des autorisations spécifiques. L'éditeur de balises ne possède ni n'utilise de rôles de service.

Utilisation d'informations d'identification temporaires avec Tag Editor

Dans Tag Editor, vous pouvez utiliser des informations d'identification temporaires pour vous connecter à la fédération, assumer un rôle IAM ou assumer un rôle multicompte. Vous obtenez des

informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

Rôles liés à un service

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

L'éditeur de balises ne possède ni n'utilise de rôles liés à un service.

Rôles du service

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

L'éditeur de balises ne possède ni n'utilise de rôles de service.

Exemples de politiques basées sur l'identité dans l'éditeur de balises

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

Pour obtenir des instructions sur la création d'une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez la section Création de politiques sur l'onglet JSON du guide de l'utilisateur IAM.

Rubriques

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

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources de l'éditeur de balises dans votre compte. Ces actions peuvent entraîner des frais pour

votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

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

Utilisation de la console Tag Editor et de l'API de balisage Resource Groups

Pour accéder à la console Tag Editor et à l'API Resource Groups Tagging, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails relatifs aux balises associées aux ressources de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, les commandes de la console et de l'API ne fonctionneront pas comme prévu pour les principaux IAM dotés de cette politique.

Pour vous assurer que ces principaux peuvent toujours utiliser l'éditeur de balises, associez la politique suivante (ou une politique contenant les autorisations répertoriées dans la politique suivante) aux entités. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

JSON

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

Pour plus d'informations sur l'octroi de l'accès à l'éditeur de balises et à l'API de balisage Resource Groups, consultezOctroi d'autorisations pour l'utilisation de l'éditeur de balises.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

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

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

Afficher les groupes en fonction des balises

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups:us-
east-1:111122223333:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups:us-
east-1:111122223333:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

Vous pouvez attacher cette stratégie aux utilisateurs de votre compte. Si un utilisateur possédant la clé de balise `project` et la valeur de balise `alpha` tente de consulter 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, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Résolution des problèmes d'identité et d'accès à l'éditeur de balises

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Tag Editor et d'IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Tag Editor
- Je ne suis pas autorisé à effectuer iam : PassRole

Je ne suis pas autorisé à effectuer une action dans Tag Editor

S'il vous Console de gestion AWS 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 balises d'une ressource mais ne dispose pas des `tag:GetTagKeys` autorisations nécessaires.

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

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

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 Tag Editor.

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, vous devez 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 Tag Editor. Toutefois, l'action nécessite que le service ait

des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre 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.

Journalisation et surveillance dans l'éditeur de balises

Toutes les actions de l'éditeur de balises sont enregistrées AWS CloudTrail.

Journalisation des appels d'API de l'éditeur de balises avec CloudTrail

L'éditeur de balises est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un éditeur Service AWS de balises intégré. CloudTrail capture tous les appels d'API pour Tag Editor sous forme d'événements, y compris les appels depuis la console Tag Editor et les appels de code vers l'API Resource Groups Tagging. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Tag Editor. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Tag Editor, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur l'éditeur de balises dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans l'éditeur de balises ou dans la console de l'éditeur de balises, cette activité est enregistrée dans un CloudTrail événement avec les autres Service AWS événements de l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre navigateur Compte AWS, y compris des événements pour Tag Editor, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Création d'un parcours pour votre Compte AWS
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions de l'éditeur de balises sont enregistrées CloudTrail et sont documentées dans la référence de l'API de l'éditeur de balises. Les actions de l'éditeur de balises dans la console sont enregistrées et affichées sous forme d'événements avec `tagging.amazonaws.com` le`eventSource`. 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 des informations d'identification d'utilisateur root ou IAM.
- Si la demande a été effectuée avec des informations d'identification 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'CloudTrail`userIdentity`élément.

Comprendre les entrées du fichier journal de l'éditeur de balises

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande individuelle à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et

l'heure, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne sont pas des séries ordonnées retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
        ],
        "tags": {
            "owner": "alice"
        }
    },
```

```
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
    }
}
```


Validation de conformité pour Tag Editor

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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Résilience dans l'éditeur de balises

Tag Editor effectue des sauvegardes automatisées des ressources du service interne. Ces sauvegardes ne sont pas configurables par l'utilisateur. Les sauvegardes sont cryptées, à la fois au repos et en transit. L'éditeur de balises stocke les données des clients dans Amazon DynamoDB.

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées,

connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Si vous supprimez des tags accidentellement, contactez le AWS Support Centre.

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

Sécurité de l'infrastructure dans Tag Editor

L'éditeur de balises ne fournit aucun autre moyen d'isoler le trafic de service ou de réseau. Le cas échéant, utilisez AWS un isolant spécifique. Vous pouvez utiliser l'API et la console Tag Editor dans un cloud privé virtuel (VPC) pour optimiser la confidentialité et la sécurité de l'infrastructure.

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

- Protocole TLS (Transport Layer Security). Nous avons besoin de TSL 1.2 et recommandons TSL 1.3.
- Des suites de chiffrement dotées d'un secret de transmission parfait (PFS), telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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 principal Gestion des identités et des accès AWS (IAM). Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

L'éditeur de balises ne prend pas en charge les politiques basées sur les ressources.

Vous pouvez appeler les opérations de l'API Tag Editor depuis n'importe quel emplacement réseau, mais Tag Editor prend en charge les politiques d'accès basées sur les ressources, qui peuvent inclure des restrictions basées sur l'adresse IP source. Vous pouvez également utiliser les politiques de l'éditeur de balises pour contrôler l'accès depuis des points de terminaison Amazon Virtual Private Cloud (Amazon VPC) spécifiques ou des VPC spécifiques. En fait, cette approche isole l'accès réseau à une ressource donnée uniquement du VPC spécifique au sein AWS du réseau.

Quotas de service

Le tableau suivant fournit des informations sur les quotas de service pour Tag Editor.

Ces quotas ne sont actuellement pas ajustables à l'aide de la console Service Quotas. Contactez Support.

Nom	Par défaut
Tags attachés par ressource	50 balises définies par l'utilisateur (les balises AWS générées ne sont pas prises en compte dans cette limite.)
Nom de la clé du tag	1 caractères Unicode au minimum et 128 caractère s Unicode au maximum en UTF-8. Les caractères autorisés incluent les lettres, les chiffres, les espaces et les caractères suivants : `_ . : / = + - @` Les noms de clé ne peuvent pas commencer par `aws:` car ce préfixe est réservé à AWS l'usage. **Note** Certains Services AWS comportent des restrictions supplémen taires en matière de caractères ou de

Nom	Par défaut
	longueur. Pour plus de détails, consultez la documentation du service concerné.
Tag Value (Valeur d'identification)	Minimum de 0, maximum de 256 caractères Unicode en UTF-8. Les caractères autorisés incluent les lettres, les chiffres, les espaces et les caractères suivants : `_ . : / = + - @` **Note** Certains Services AWS comportent des restrictions supplémentaires en matière de caractères ou de longueur. Pour plus de détails, consultez la documentation du service concerné.
Taux d'appel GetResourcesOpération d'API	Maximum de 15 appels par seconde

Nom	Par défaut	
Taux d'appel des opérations d'API suivantes : • TagResources • UntagResources • GetTagKeys • GetTagValues	Maximum de 5 appels par seconde	

Historique du document Tag Editor

Modification	Description	Date
Autorisations mises à jour pour évaluer la conformité à l'échelle de l'organisation	Mise à jour des autorisations pour évaluer la conformité à l'échelle de l'organisation afin d'inclure des autorisations facilitant l'accès au rapport de conformité.	28 août 2024
Contenu mis à jour	Titres de sujets mis à jour et contenu réorganisé pour améliorer la lisibilité et la découvrabilité.	25 juillet 2024
Marquer le contenu depuis son Références générales AWS transfert vers ce guide	Les rubriques relatives au balisage de vos AWS ressources ont été déplacées du Références générales AWS présent guide.	24 mars 2023
Mise à jour des meilleures pratiques IAM	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	3 janvier 2023
Transférer la documentation de l'éditeur de balises vers son propre guide	La documentation de Tag Editor est désormais fournie dans son propre guide de l'utilisateur au lieu de faire partie du guide de Groupes de ressources AWS l'utilisateur.	13 décembre 2022
Vérifier la conformité aux politiques relatives aux balises	Une fois que vous avez créé et associé des politiques de	26 novembre 2019

	balises aux comptes à l'aide de celles-ci AWS Organizations, vous pouvez trouver des balises non conformes sur les ressources des comptes de votre organisation.	
L'éditeur de balises permet désormais de rechercher des ressources non étiquetées	Vous pouvez désormais rechercher des ressources dans l'éditeur de balises auxquelles aucune valeur de balise n'est appliquée pour une clé de balise spécifique.	18 juin 2019
La console Tag Editor quitte la AWS Systems Manager console	La console Tag Editor est désormais indépendante de la console Systems Manager. Bien que vous puissiez toujours trouver des pointeurs vers la console Tag Editor dans la barre de navigation gauche de Systems Manager, vous pouvez ouvrir la console Tag Editor directement depuis le menu déroulant en haut à gauche du Console de gestion AWS.	5 juin 2019
Les anciens outils d'édition de balises ne sont plus disponibles	Les mentions d'un éditeur de balises ancien, classique ou ancien ont été supprimées ; ces outils ne sont plus disponibles dans AWS. Utilisez plutôt l'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'exportation des résultats des requêtes vers un fichier CSV	Vous pouvez exporter les résultats d'une requête sur la page Find Resources to tag (Rechercher des ressources à baliser) vers un fichier au format CSV. 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

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.