Guia do usuário

Recursos de marcação AWS

Versão 1.0

Recursos de marcação AWS: Guia do usuário

Table of Contents

Marcando seus Recursos AWS

As tags são pares de chave e valor que atuam como metadados para organizar seus recursos da AWS. Com a maioria dos recursos da AWS, você tem a opção de adicionar tags ao criar o recurso. Exemplos de recursos incluem uma instância do Amazon Elastic Compute Cloud (Amazon EC2), um bucket do Amazon Simple Storage Service (Amazon S3) ou um segredo no AWS Secrets Manager.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. Usamos tags para fornecer serviços de cobrança e administração. As tags não devem ser usadas para dados privados ou confidenciais.

As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios.

Cada tag tem duas partes:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). Chaves de tag fazem distinção entre maiúsculas e minúsculas.
- Um valor de tag (por exemplo, `111122223333` ou `Production`). Como chaves de tag, os valores das tags diferenciam maiúsculas de minúsculas.

Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios.

Como adicionar tags aos seus recursos da AWS

Há três maneiras de adicionar tags aos seus recursos da AWS:

- Operação de API do AWS service (Serviço da AWS): as operações de API de atribuição de tags oferecem suporte diretamente a um AWS service (Serviço da AWS). Para descobrir qual funcionalidade de atribuição de tag cada AWS service (Serviço da AWS) fornece, consulte a documentação do serviço no Índice de documentação da AWS.
- Console do Tag Editor: alguns serviços também oferecem suporte à atribuição de tags com o console do Tag Editor da AWS.

- API de marcação de grupos de recursos: a maioria dos serviços também oferece suporte à atribuição de tags usando o AWS Resource Groups Tagging API.

É possível etiquetar recursos para todos os serviços que aumentam os custos na AWS. Para os serviços a seguir, a AWS recomenda Serviços da AWS alternativos mais novos que ofereçam suporte à marcação para melhor atender aos casos de uso de clientes.

Amazon Cloud Directory	Amazon CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon S3 Glacier Direct	Amazon SimpleDB
Gerenciador WorkSpaces de aplicativos da Amazon	AWS DeepLens	

Práticas recomendadas

À medida que você cria uma estratégia de marcação para recursos da AWS, siga as melhores práticas:

- Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos serviços da AWS, incluindo faturamento. As tags não devem ser usadas para dados privados ou confidenciais.
- Use um formato padronizado que diferencia maiúsculas de minúsculas para tags e aplique-o de forma consistente a todos os tipos de recursos.
- Considere as diretrizes de tags que oferecem suporte a diversas finalidades, como gerenciar o controle de acesso a recursos, o rastreamento de custos, a automação e a organização.
- Use ferramentas automatizadas para ajudar a gerenciar as tags de recursos. O Tag Editor e a API de marcação de grupos de recursos capacitam o controle programático de tags, tornando fácil gerenciar, pesquisar e filtrar tags e recursos automaticamente.
- Use muitas tags em vez de muito poucas.
- Lembre-se de que é fácil alterar tags para acomodar os requisitos de negócios em constante mudança, mas considere as consequências de mudanças futuras. Por exemplo, alterar tags de controle de acesso significa que você também deve atualizar as políticas que fazem referência a essas tags e controlar o acesso aos recursos.

- É possível aplicar automaticamente os padrões de marcação que sua organização escolher adotar criando e implantando políticas de etiquetas com o AWS Organizations. As políticas de etiquetas permitem especificar regras de marcação que definem nomes de chave válidos e os valores que são válidos para cada chave. É possível optar por apenas monitorar, dando a você a oportunidade de avaliar e limpar suas etiquetas existentes. Quando suas etiquetas estiverem em conformidade com os padrões escolhidos, você poderá ativar a imposição nas políticas de etiquetas para evitar a criação de etiquetas não compatíveis. Para obter mais informações, consulte Políticas de etiquetas no Guia do usuário do AWS Organizations.

Categorias de marcação

As empresas que apresentam maior eficiência no uso de tags geralmente criam agrupamentos de tags relevantes para o negócio, a fim de organizar os recursos nas dimensões técnicas, comerciais e de segurança. As empresas que usam processos automatizados para gerenciar a infraestrutura também incluem tags adicionais específicas para automação.

Etiquetas técnicas	Tags para automação	Etiquetas comerciais	Etiquetas de segurança
• Nome – identifica recursos individuais • ID do aplicativo – identifica recursos relacionados a um aplicativo específico • Função do aplicativo – descreve a função de um recurso específico (como servidor Web, agente de mensagens, banco de dados) • Cluster – identifica farms de recursos que compartilham	• Data/hora – identifica a data ou a hora em que um recurso deve ser iniciado, interrompido, excluído ou alternado • Aceitar/recusar – indica se um recurso deve ser incluído em uma atividade automatizada, como iniciar, interromper ou redimensionar instâncias	• Projeto – identifica projetos compatíveis com o recurso • Proprietário – identifica o responsável pelo recurso • Centro de custo/unidade de negócios – identifica o centro de custo ou a unidade de negócios associada a um recurso, normalmente para alocação e	• Confidencialidade – um identificador para o nível de confidencialidade de dados específico compatível com um recurso. • Conformidade – um identificador de cargas de trabalho que devem aderir a requisitos de conformidade específicos

Etiquetas técnicas	Tags para automação	Etiquetas comerciais	Etiquetas de segurança
uma configuração comum e executam uma função específica para um aplicativo • Ambiente – diferencia recursos de desenvolvimento, teste e produção • Versão – ajuda a distinguir entre versões de recursos ou aplicativos	• Segurança: determina requisitos, como criptografia ou habilitação de logs de fluxo da Amazon VPC; identifica tabelas de rotas ou grupos de segurança que precisam de análise adicional	rastreamento de custos • Cliente – identifica um cliente específico atendido por um grupo de recursos específico	

Limites e requisitos de nomenclatura de tags

Os seguintes requisitos básicos de uso e de nomenclatura e se aplicam às tags:

- Cada recurso pode ter no máximo 50 tags criadas pelo usuário.
- As tags criadas pelo sistema que começam com `aws:` são reservadas para uso da AWS e não contam em relação a esse limite. Não é possível editar nem excluir uma tag que começa com o prefixo `aws:`.
- Em todos os recursos, cada chave de tag deve ser exclusiva e pode ter apenas um valor.
- A chave de tag deve ter no mínimo 1 e no máximo 128 caracteres Unicode em UTF-8.
- O valor da tag deve ter no mínimo 0 e no máximo de 256 caracteres Unicode em UTF-8.
- Os caracteres permitidos podem variar de acordo com o serviço da AWS. Para obter mais informações sobre quais caracteres podem ser usados para marcar recursos em um serviço específico da AWS, consulte a respectiva documentação. Em geral, os caracteres permitidos são letras, números, espaços representáveis em UTF-8 e os seguintes caracteres: _ . : / = + - @.

- As chaves e valores das tags diferenciam maiúsculas de minúsculas. Como melhor prática, adote uma estratégia para letras maiúsculas em tags e implemente-a de forma consistente em todos os tipos de recursos. Por exemplo, decida se deseja usar `Costcenter`, `costcenter` ou `CostCenter` e use a mesma convenção para todas as tags. Evite usar tags semelhantes com tratamento do tamanho de letra inconsistente.

Estratégias comuns de marcação

Use as estratégias de marcação a seguir para ajudar a identificar e gerenciar recursos da AWS.

Conteúdo

Tags para organização de recursos

As tags são uma ótima forma de organizar recursos da AWS no AWS Management Console. É possível configurar tags para serem exibidas com recursos, além de pesquisar e filtrar por tags. Com o serviço do AWS Resource Groups, é possível criar grupos de recursos da AWS com base em uma ou mais tags ou partes de tags. Também é possível criar grupos baseados em ocorrência em uma pilha do AWS CloudFormation. Usando o Resource Groups e o Tag Editor, é possível consolidar e visualizar dados de aplicações que consistem em múltiplos serviços, recursos e regiões em um só lugar.

Tags para alocação de custos

O AWS Cost Explorer e os relatórios de faturamento detalhados permitem dividir os custos da AWS por tag. Normalmente, você usa tags de negócios como centro de custo/unidade de negócios, cliente ou projeto para associar custos da AWS a dimensões tradicionais de alocação de custos. Porém, um relatório de alocação de custos pode incluir qualquer tag. Isso permite associar custos a dimensões técnicas ou de segurança, como aplicativos, ambientes ou programas de conformidade específicos. Veja a seguir um exemplo de um relatório de alocação de custos parcial.

Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal
2.47	DbAdmin	Prod	78925	Portal

Para alguns serviços, é possível usar uma tag AWS gerada pela `createdBy` para fins de alocação de custos, para ajudar a contabilizar recursos que podem não ter sido categorizados. A tag `createdBy` está disponível apenas para serviços e recursos compatíveis com a AWS. O valor contém dados associados a uma API específica ou a eventos do console. Para obter mais informações, consulte Tags de alocação de custos geradas pela AWS noGuia do usuário do AWS Billing and Cost Management.

Tags para automação

As tags específicas de recursos ou serviços são geralmente usadas para filtrar recursos durante atividades de automação. As tags de automação são usadas para aceitar ou recusar tarefas automatizadas ou para identificar versões específicas de recursos para arquivar, atualizar ou excluir. Por exemplo, é possível executar scripts `start` ou `stop` automatizados que desativam ambientes de desenvolvimento fora do horário comercial para reduzir custos. Nesse cenário, as etiquetas de instância do Amazon Elastic Compute Cloud (Amazon EC2) são uma forma simples de identificar instâncias para recusar essa ação. Para scripts que localizam e excluem snapshots obsoletos ou contínuos do Amazon EBS, as tags de snapshot podem adicionar uma dimensão extra aos critérios de pesquisa. out-of-date

Tags para controle de acesso

As políticas do IAM oferecem suporte a condições baseadas em etiquetas, permitindo restringir permissões do IAM com base em etiquetas ou em valores de etiquetas específicos. Por exemplo, as permissões de usuário ou perfil do IAM podem incluir condições para limitar as chamadas de API do EC2 para ambientes específicos (como desenvolvimento, teste ou produção) com base nas etiquetas. A mesma estratégia pode ser usada para limitar chamadas de API para redes específicas da Amazon Virtual Private Cloud (Amazon VPC). O suporte para permissões do IAM baseadas em etiquetas no nível de recursos é específico para o serviço. Ao usar condições baseadas em tags para controle de acesso, certifique-se de definir e restringir quem pode modificar as tags. Para obter mais

informações sobre como usar tags para controlar o acesso da API aos recursos da AWS, consulte Serviços da AWS que operam com o IAM no Guia do usuário do IAM.

Governança de marcação

Uma estratégia de marcação eficiente usa tags padronizadas e as aplica de forma consistente e programática em todos os recursos da AWS. É possível usar abordagens reativas e proativas para tags de governança no ambiente da AWS.

- A Governança reativa é para encontrar recursos que não são marcados corretamente usando ferramentas, como a API de marcação do grupo de recursos, Regras do AWS Config e scripts personalizados. Para localizar recursos manualmente, é possível usar o Editor de tags e os relatórios de faturamento detalhado.
- A governança proativa usa ferramentas como o AWS CloudFormation, o Service Catalog, as políticas de etiquetas no AWS Organizations ou as permissões no nível de recursos do IAM para garantir que as etiquetas padronizadas sejam aplicadas de forma consistente na criação dos recursos.

  Por exemplo, é possível usar a propriedade AWS CloudFormation do `Resource Tags` para aplicar tags aos tipos de recursos. No Service Catalog, é possível adicionar etiquetas de portfólio e de produto que são combinadas e aplicadas a um produto automaticamente quando ele é iniciado. As formas mais rigorosas de governança proativa incluem tarefas automatizadas. Por exemplo, é possível usar a API de marcação de grupos de recursos para pesquisar tags do ambiente da AWS ou executar scripts para colocar recursos marcados incorretamente em quarentena ou para excluí-los.

Saiba mais

Esta página fornece informações gerais sobre os recursos de marcação da AWS. Para obter mais informações sobre os recursos de marcação em um serviço específico da AWS, consulte a respectiva documentação. Veja a seguir outras fontes de informações sobre marcação:

- Para obter informações sobre o AWS Resource Groups Tagging API, consulte o Guia de referência da API do Resource Groups Tagging.
- Para obter mais informações sobre o Tag Editor, consulte Tag Editor neste guia.
- Para obter informações sobre a funcionalidade de marcação que cada AWS service (Serviço da AWS) fornece, consulte a documentação do serviço no Índice de documentação da AWS.

- Para obter informações sobre o uso de tags em políticas do IAM para ajudar a controlar quem pode visualizar e interagir com seus recursos da AWS, consulte Controle de acesso para usuários e perfis do IAM que usam tags no Guia do usuário do IAM.

Usar o Tag Editor

As tags são pares de chave e valor que atuam como metadados para organizar seus recursos da AWS. Com a maioria dos recursos da AWS, você tem a opção de adicionar tags ao criar o recurso. Exemplos de recursos incluem uma instância do Amazon Elastic Compute Cloud (Amazon EC2), um bucket do Amazon Simple Storage Service (Amazon S3) ou um segredo no AWS Secrets Manager. No entanto, você também pode adicionar tags a vários recursos com suporte de uma vez usando o Tag Editor. Você cria uma consulta de recursos de vários tipos e adiciona, remove ou substitui as tags dos recursos nos resultados da pesquisa. As consultas atribuem um operador `AND` às tags, de forma que qualquer recurso que corresponda aos tipos de recurso especificados e todas as tags especificadas seja retornado pela consulta.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. Usamos tags para fornecer serviços de cobrança e administração. As tags não devem ser usadas para dados privados ou confidenciais.

Para adicionar tags (ou editar ou excluir tags) a vários recursos de uma vez, use o Tag Editor. Com o Tag Editor, você pode pesquisar os recursos que deseja marcar e gerenciar as tags dos recursos nos resultados da pesquisa.

Para iniciar o Tag Editor

1. Faça login no AWS Management Console.
2. Execute uma das seguintes etapas:
   - Selecione Serviços. Em seguida, em Gerenciamento e governança, escolha Grupos de recursos e Tag Editor. No painel de navegação à esquerda, escolha Tag Editor.
   - Use o link direto:Console do Tag Editor da AWS.

Nem todos os recursos podem ter tags aplicadas. Para obter informações sobre quais recursos o Tag Editor oferece suporte, consulte a coluna de marcação do Tag Editor em Tipos de recursos compatíveis no Guia do usuário do AWS Resource Groups. Se um tipo de recurso que você deseja marcar não for compatível, informe a AWS, escolhendo a ferramenta Feedback no canto inferior esquerdo da janela do console.

Para obter informações sobre as permissões e funções necessárias para marcar recursos, consulte Configurar permissões.

Tópicos

Tags e controle de acesso baseado em atributo

As tags podem ser uma parte importante da sua estratégia de controle de acesso da AWS. Para obter informações sobre o uso de tags como atributos em uma estratégia de controle de acesso por atributo (ABAC), consulte Controlar o acesso a recursos da AWS usando tags e Controlar o acesso a usuários e perfis do IAM usando tags, ambos no Guia do usuário do IAM.

Há um tutorial abrangente que mostra como conceder acesso a diferentes projetos e grupos usando tags no Tutorial do IAM: Definir permissões para acessar recursos da AWS com base em tags no Guia do usuário do AWS Identity and Access Management.

Se você usar um provedor de identidades (IdP) baseado em SAML para login único, você pode anexar tags aos perfis assumidos que fornecem acesso aos seus usuários. Para obter mais informações, consulte Tutorial do IAM: usar tags de sessão SAML para ABAC no Guia do usuário do AWS Identity and Access Management.

Práticas recomendadas de nomes de tags

Estas são algumas práticas recomendadas e convenções de nomenclatura que recomendamos usar com suas tags.

Os nomes de chaves para tags da AWS diferenciam maiúsculas de minúsculas. Portanto, verifique se elas são usadas de forma consistente. Por exemplo, as chaves de tags `CostCenter` e `costcenter` são diferentes. Uma chave de tag pode ser configurada como uma tag de alocação de custos para análise financeira e relatórios, e a outra chave de tag pode não ser configurada para o mesmo uso.

Várias tags são predefinidas pela AWS ou criadas automaticamente por diversos Serviços da AWS. Muitas tags geradas da AWS usam nomes de chaves que usam todas as letras minúsculas, com hifens separando palavras no nome e prefixos seguidos por dois pontos para identificar o serviço de origem da tag. Por exemplo, consulte:

- `aws:ec2spot:fleet-request-id` é uma tag que identifica a solicitação de instância spot do Amazon EC2 que iniciou a instância.
- `aws:cloudformation:stack-name` é uma tag que identifica a pilha AWS CloudFormation que criou o recurso.
- `elasticbeanstalk:environment-name` é uma tag que identifica a aplicação que criou o recurso.

Considere nomear suas tags usando as seguintes regras:

- Use todas as letras minúsculas para as palavras.
- Use hífens para separar palavras.
- Use um prefixo seguido por dois pontos para identificar o nome da organização ou o nome abreviado.

Por exemplo, para uma empresa fictícia chamada AnyCompany, você pode definir tags como:

- `anycompany:cost-center` para identificar o código interno do centro de custos.
- `anycompany:environment-type` para identificar se o ambiente é de desenvolvimento, teste ou produção.
- `anycompany:application-id` para identificar a aplicação para a qual o recurso foi criado.

O prefixo garante que as tags sejam claramente reconhecíveis como tendo sido definidas pela sua organização, e não pela AWS nem por uma ferramenta de terceiros que você possa estar usando. Usar todas as letras minúsculas com hifens para separadores evita confusão sobre como formatar o nome de uma etiqueta em letras maiúsculas. Por exemplo, `anycompany:project-`

`id` é mais simples de lembrar do que `ANYCOMPANY:ProjectID`, `anycompany:projectID` ou `Anycompany:ProjectId`.

Conceitos básicos sobre o Tag Editor

O Tag Editor é uma forma de marcar seus recursos. Veja as seções abaixo para entender os pré-requisitos que você deve satisfazer para usá-lo.

Pré-requisitos para trabalhar com o Tag Editor

Antes de começar a trabalhar para marcar seus recursos, tenha uma Conta da AWS ativa com recursos existentes e direitos apropriados para marcar recursos e criar grupos.

Tópicos

- Inscreva-se para um Conta da AWS
- Criar um usuário administrativo
- Criar recursos do
- Configurar permissões

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Acesse https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Durante a criação da conta, você vai receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e utilize somente o usuário raiz para executar as tarefas que exigem acesso do usuário raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário doInício de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário doAWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no GuiaAWS IAM Identity Center do usuário.

Login como usuário administrativo

- Para fazer login com o usuário do Centro de Identidade do IAM, utilize o URL de login enviado ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no GuiaInício de Sessão da AWS do usuário.

Criar recursos do

Você deve ter recursos em sua tag Conta da AWS to. Para obter mais informações sobre os tipos de recursos compatíveis, consulte a coluna Marcação do Tag Editor em Tipos de recursos com suporte no Guia do usuário doAWS Resource Groups .

Configurar permissões

Para aproveitar ao máximo o Tag Editor, você talvez precise de permissões adicionais para marcar recursos ou para ver as chaves e valores de tag de um recurso. Essas permissões se encaixam nas seguintes categorias:

- Permissões para serviços individuais, para que você possa marcar recursos desses serviços e incluí-los em grupos de recursos.
- Permissões que são necessárias para usar o console do Tag Editor.

Se você for administrador, poderá fornecer permissões para seus usuários criando políticas por meio do serviço AWS Identity and Access Management (IAM). Primeiro, crie grupos, usuários ou perfis do IAM e, em seguida, aplique as políticas com as permissões que eles precisam. Para obter informações sobre como criar e anexar políticas do IAM, consulte Como trabalhar com políticas.

Permissões para serviços individuais

> **Important**
>
> Esta seção descreve as permissões necessárias se você quiser marcar recursos de outros consoles de AWS serviço e APIs.

Para adicionar tags a um recurso, você precisa das permissões necessárias para o serviço ao qual o recurso pertence. Por exemplo, para marcar instâncias do Amazon EC2, você deve ter permissões para as operações de marcação na API desse serviço, como a operação do Amazon EC2 CreateTags.

Permissões necessárias para usar o console do Editor de tags

Para usar o console do Editor de tags para listar e marcar recursos, as seguintes permissões devem ser adicionadas à declaração de política do usuário no IAM. Você pode adicionar políticas AWS gerenciadas que são mantidas e AWSatualizadas ou criar e manter sua própria política personalizada.

Usando políticas AWS gerenciadas para permissões do Editor de tags

O Tag Editor oferece suporte às seguintes políticas AWS gerenciadas que você pode usar para fornecer um conjunto predefinido de permissões aos seus usuários. Você pode anexar essas políticas gerenciadas a qualquer perfil, usuário ou grupo da mesma forma que faria com qualquer outra política criada por você.

ResourceGroupsandTagEditorReadOnlyAccess

Essa política concede ao papel do IAM ou ao usuário anexado permissão para chamar as operações somente de leitura tanto para o Editor de tags AWS Resource Groups quanto para o Editor de tags. Para ler as tags de um recurso, você também deve ter permissões para esse recurso por meio de uma política separada. Saiba mais na seguinte nota importante.

ResourceGroupsandTagEditorFullAccess

Essa política concede ao usuário e perfil do IAM anexado permissão para chamar qualquer operação do Resource Groups e as operações de tag de leitura e gravação no Tag Editor. Para ler ou gravar as tags de um recurso, você também deve ter permissões para esse recurso por meio de uma política separada. Saiba mais na seguinte nota importante.

Important

As duas políticas anteriores concedem permissão para chamar as operações do Tag Editor e usar o console do Tag Editor. No entanto, você também deve ter permissões não apenas para invocar a operação, mas também permissões apropriadas para o recurso específico cujas tags você está tentando acessar. Para conceder esse acesso às tags, é necessário anexar uma das seguintes políticas:

- A política AWS gerenciada ReadOnlyAccessconcede permissões para as operações somente de leitura dos recursos de cada serviço. AWS mantém automaticamente essa política atualizada com as novas à Serviços da AWS medida que elas se tornam disponíveis.

- Muitos serviços fornecem políticas AWS gerenciadas somente para leitura específicas que você pode usar para limitar o acesso somente aos recursos fornecidos por esse serviço. Por exemplo, o Amazon EC2 fornece AmazonEC2ReadOnlyAccess.
- Você pode criar sua própria política que conceda acesso somente às operações somente leitura específicas para os poucos serviços e recursos que você deseja que seus usuários acessem. Essa política usa uma estratégia de lista de permissões ou lista de negação.

  Uma estratégia de lista de permissões aproveita o fato de que o acesso é negado por padrão até que você o permita explicitamente em uma política. Portanto, você pode usar uma política como o exemplo a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
}
```

  Como alternativa, você pode usar uma estratégia de lista de negação que permita acesso a todos os recursos, exceto aqueles que você bloqueia explicitamente. Isso requer uma política separada que se aplique aos usuários relevantes e que permita o acesso. O exemplo de política a seguir nega o acesso aos recursos específicos listados pelo nome do recurso da Amazon (ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to disallow tagging>"
        }
    ]
}
```

Adicionar permissões do Tag Editor manualmente

- `tag:*` (Essa permissão permite todas as ações do Tag Editor. Se, em vez disso, quiser restringir as ações que estão disponíveis para um usuário, você pode substituir o asterisco por uma ação específica ou por uma lista de ações separadas por vírgulas.)
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **Note**
>
> A `resource-groups:SearchResources` permissão permite que o Editor de tags liste recursos quando você filtra sua pesquisa usando chaves ou valores de tag.
> A `resource-explorer:ListResources` permissão permite que o Editor de tags liste recursos quando você pesquisa recursos sem definir tags de pesquisa.

Conceder permissões para usar o Tag Editor

Para adicionar uma política de uso AWS Resource Groups do Editor de tags a uma função, faça o seguinte.

1. Abra o console do IAM na página Perfis.
2. Encontre o perfil ao qual você deseja conceder as permissões do Tag Editor. Escolha o nome do perfil para abrir a página Resumo do perfil.
3. Na guia Permissões, escolha AAdicionar permissões.
4. Escolha Anexar políticas existentes diretamente.
5. Escolha Criar política.
6. Na guia JSON, cole a seguinte declaração de política.

```
{
  "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**
>
> Esta declaração de política concede permissões somente para ações do Tag Editor.

7. Escolha Próximo: etiquetas e Próximo: revisar.
8. Digite um nome e uma descrição para a nova política. Por exemplo, **`AWSTaggingAccess`**.
9. Escolha Criar política.

Agora que a política está salva no IAM, você pode vinculá-la a outras entidades principais, como perfis, grupos ou usuários. Para obter informações sobre como adicionar uma política a uma entidade principal, consulte Adicionar e remover permissões de identidade do IAM no Guia do usuário do IAM.

Autorização e controle de acesso com base em tags

Serviços da AWS apoie o seguinte:

- Políticas baseadas em ações: por exemplo, você pode criar uma política que permita que os usuários executem operações `GetTagKeys` ou `GetTagValues`, mas não outras.

- Permissões no nível do recurso: muitos serviços oferecem suporte ao uso de ARNs para especificar recursos individuais na política.
- Autorização baseada em tags: muitos serviços oferecem suporte ao uso de tags de recurso na condição de uma política. Por exemplo, você pode criar uma política que conceda a usuários acesso total a um grupo que possui a mesma tag dos usuários. Para obter mais informações, consulte Para que serve o ABAC? AWSno Guia doAWS Identity and Access Management usuário.
- Credenciais temporárias: os usuários podem assumir um perfil com uma política que permita operações do Tag Editor.

O Tag Editor não usa perfis vinculados a serviço.

Para obter mais informações sobre como o Tag Editor se integra ao AWS Identity and Access Management (IAM), consulte os tópicos a seguir no Guia doAWS Identity and Access Management usuário:

- AWS serviços que funcionam com o IAM
- Ações, recursos e chaves de condição para o Tag Editor
- Controle de acesso aos recursos da AWS usando políticas

Como encontrar recursos para marcar

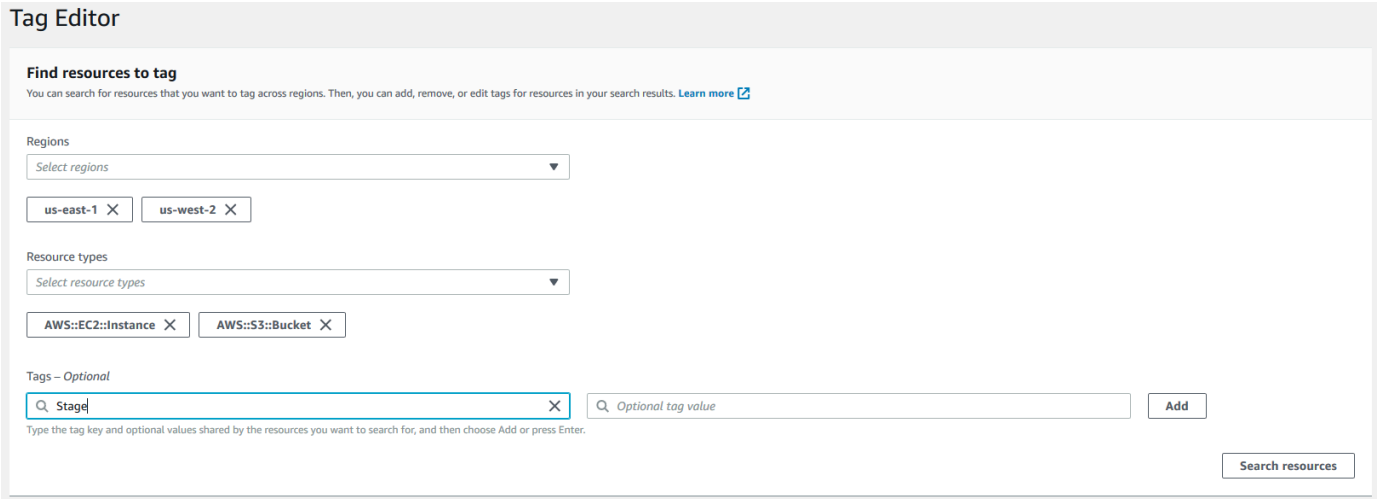
Com o Tag Editor, você cria uma consulta para encontrar recursos em uma ou mais Regiões da AWS disponíveis para marcação. Você pode escolher até 20 tipos de recurso individual ou criar uma consulta em Todos os tipos de recurso. Sua consulta pode incluir recursos que já têm tags ou recursos que não têm tags. Para obter mais informações, consulte a coluna Marcação do Tag Editor em Tipos de recursos compatíveis no Guia do usuário do AWS Resource Groups.

Depois de encontrar recursos para marcar, você pode usar o Tag Editor para adicionar tags ou visualizar, editar ou excluir tags.

Para encontrar recursos para marcar

1. Abra o console do Tag Editor.
2. (Opcional) Escolha as Regiões da AWS onde pesquisar recursos para marcar. Por padrão, sua região atual é selecionada. Para este procedimento, escolha us-east-1 e us-west-2.

3. Escolha pelo menos um tipo de recurso na lista suspensa Tipos de recurso. Você pode adicionar ou editar tags para até 20 tipos de recurso individual por vez, ou escolher Todos os tipos de recurso. Para este procedimento, escolha AWS::EC2::InstanceAWS::S3::Buckete.



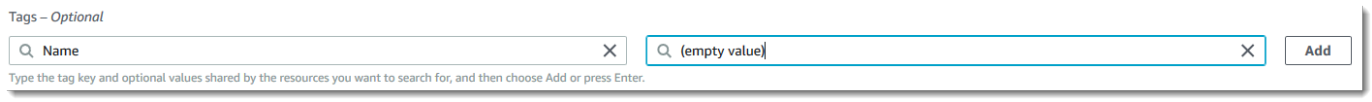
4. (Opcional) Nos campos Tags, digite uma chave de tag ou um par de chave e valor de tags para limitar os recursos na Região da AWS atual a apenas os que estão marcados com os valores especificados. Quando você digita uma chave de tag, as chaves de tag correspondentes na região atual aparecem em uma lista abaixo. É possível escolher uma chave de tag na lista. O Tag Editor preenche automaticamente a chave de tag à medida que você digita caracteres suficientes para corresponder a uma chave existente. Escolha Adicionar ou pressione Enter quando tiver concluído a tag. Neste exemplo, filtramos os recursos que têm uma chave de tag Stage (Estágio). O valor da tag é opcional, mas restringe ainda mais os resultados da consulta. Para adicionar mais tags, escolha Adicionar. As consultas atribuem um operador `AND` às tags, de forma que qualquer recurso que corresponda ao tipo de recurso especificado e a todas as tags especificadas seja retornado pela consulta.

> **Note**
>
> No momento, o console do Tag Editor não oferece suporte a curingas.

Para encontrar recursos com vários valores para uma chave de tag, adicione outra tag com a mesma chave à consulta, mas especifique um valor diferente. Os resultados incluem todos os recursos marcados com a mesma chave de tag e que têm qualquer um dos valores selecionados. A pesquisa diferencia maiúsculas de minúsculas.

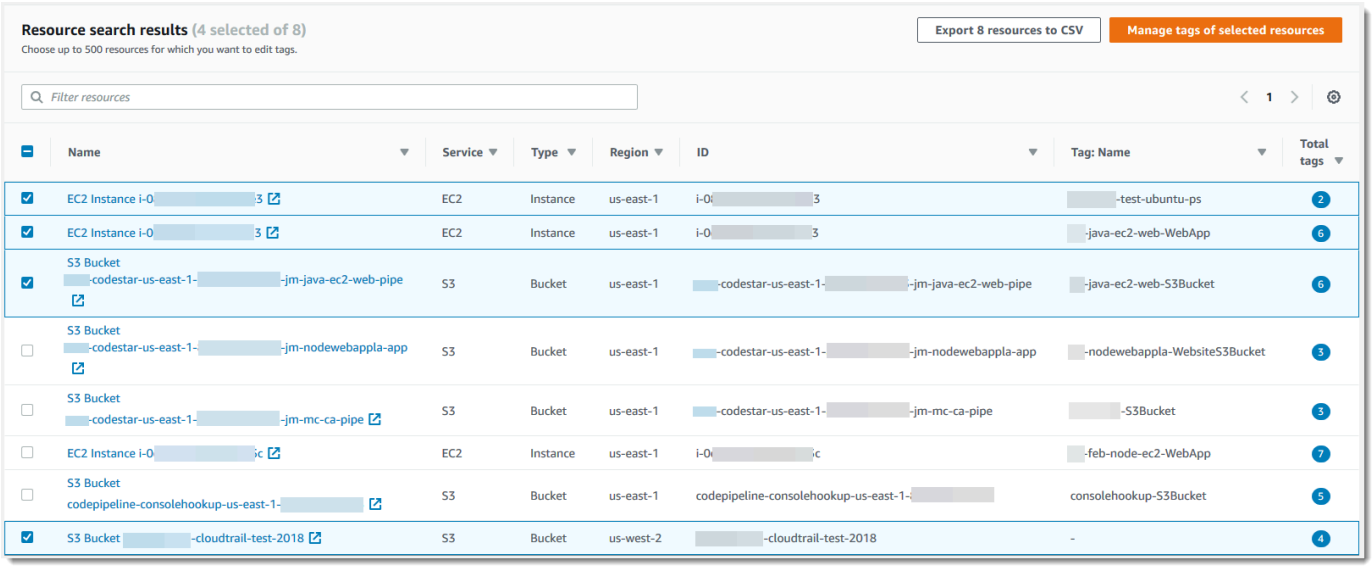
Deixe as caixas Tags em branco para encontrar todos os recursos do tipo especificado nas Regiões da AWS selecionadas. Essa consulta retorna recursos com qualquer tag e inclui os que não têm tags. Para remover uma tag da consulta, escolha X no rótulo da tag.

Para encontrar recursos que tenham uma tag, mas com um valor vazio, escolha (valor vazio), conforme mostrado abaixo, quando o cursor estiver na caixa de valor da tag.



> **Note**
>
> Para poder encontrar recursos com as tags especificadas, elas devem ter sido aplicadas a pelo menos um recurso do tipo especificado na Região da AWS atual.

5. Quando a consulta estiver pronta, escolha Pesquisar recursos. Os resultados são exibidos como uma tabela na área Resultados da pesquisa de recursos.



Para filtrar um grande número de recursos, insira qualquer texto de filtro, como parte do nome de um recurso, em Filtrar recursos.

> **Note**
>
> Você pode usar substrings para filtrar seus resultados.

6. (Opcional) Para configurar as colunas que o Tag Editor exibe nos resultados da pesquisa de recursos, escolha o ícone de engrenagem Preferências

   nos Resultados da pesquisa de recursos.

   Na página Preferências, escolha o número de linhas a serem exibidas nos resultados de pesquisa. Se você quiser ver todo o texto na tabela, marque a caixa de seleção Quebrar linhas.

   Ative as colunas que você deseja que o Tag Editor exiba nos resultados. Você pode mostrar colunas para cada tag que ocorre nos resultados da pesquisa ou um subconjunto selecionado dos resultados da pesquisa. Você pode fazer isso a qualquer momento após encontrar os recursos a serem marcados. Para ativar uma coluna, escolha o ícone de alternância ao lado da tag e altere-o de desativado

   para ativado

   .

   Ao concluir a configuração das colunas visíveis e o número de linhas exibidas, escolha Confirmar.

Exibir e editar tags para um recurso selecionado

O Tag Editor mostra as tags existentes em recursos selecionados nos resultados da consulta Encontrar recursos para marcar.

Se você ativou qualquer coluna Tag conforme descrito na seção anterior, poderá ver o valor atual dessa tag para cada recurso nos resultados da pesquisa.

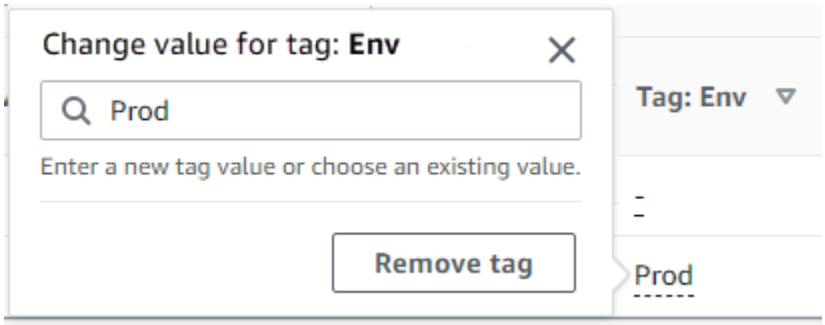
> **Note**
>
> Este tópico explica como editar a tag de um recurso individual. Você também pode editar em massa as tags de vários recursos selecionados ao mesmo tempo. Para ter mais informações, consulte Gerenciar tags com o Tag Editor.

Para editar tags em linha na tabela de resultados da pesquisa

1. Escolha o valor da tag no recurso que você deseja editar.

> **Note**
>
> - Se o recurso escolhido atualmente não tiver uma tag com a chave escolhida, o valor será exibido como (não marcado).
> - Se o recurso escolhido tiver uma tag com a chave escolhida, mas sem um valor, o valor será exibido como “–”.

No exemplo a seguir, a coluna para a tag Env e com o valor atual de Prod foi escolhida.



2. Você pode inserir um novo valor ou escolher qualquer um dos valores já presentes em outros recursos com essa tag. Você também pode excluir a tag desse recurso escolhendo Remover tag.

Para visualizar todas as tags de um recurso individual

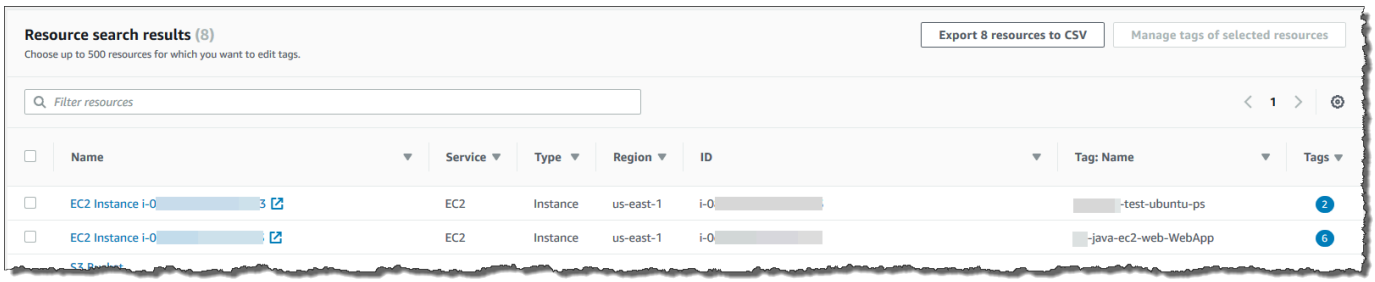
1. Nos resultados da consulta Encontrar recursos para marcar, escolha o número na coluna Tags de qualquer recurso para o qual você deseja visualizar as tags existentes. Recursos com um traço na coluna Tags (Tags) não têm tags existentes.
2. Visualize as tags existentes em Tags de recursos. Você também pode abrir essa janela escolhendo Gerenciar tags de recursos selecionados ao alterar ou remover tags da página Gerenciar tags.

> **Note**
>
> Se uma tag recém-aplicada a um recurso não estiver visível, tente atualizar a janela do navegador.

Exportar os resultados para arquivo .csv

Você pode exportar os resultados de uma consulta Encontrar recursos para marcar para um arquivo de valores separados por vírgulas (.csv). O arquivo .csv inclui os nomes dos recursos, serviços, região, IDs de recursos, o número total de tags e uma coluna para cada chave de tag exclusiva na coleção. O arquivo .csv pode ajudar a desenvolver uma estratégia de marcação dos recursos de sua organização ou determinar onde há sobreposições ou inconsistências na marcação dos recursos.

1. Nos resultados da consulta Encontrar recursos para marcar, escolha Exportar recursos para CSV.



2. Quando solicitado pelo seu navegador, escolha abrir o arquivo .csv ou salve-o em um local conveniente.

Informações relacionadas

- Usar tags de alocação de custos no Guia do usuário do AWS Billing

Gerenciar tags com o Tag Editor

Depois de ter encontrado os recursos que deseja marcar, você pode adicionar, remover e editar as tags para alguns ou todos os resultados da pesquisa. O Tag Editor mostra todas as tags anexadas aos recursos. Também mostra se essas tags foram adicionadas no Tag Editor, pelo console de serviço do recurso ou usando a API.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. Usamos tags para fornecer serviços de cobrança e administração. As tags não devem ser usadas para dados privados ou confidenciais.

Outras formas de gerenciar suas tags

Este tópico discute recursos de atribuição de tags usando o Tag Editor no AWS Management Console. No entanto, você também pode gerenciar as tags em seus recursos da AWS usando as seguintes ferramentas:

- Você pode digitar ou programar comandos no prompt do shell usando os comandos da `resourcegroupstaggingapi` no AWS Command Line Interface (AWS CLI).
- Você pode criar e executar scripts PowerShell usando a API de atribuição de tags do AWS Resource Groups no AWS Tools for PowerShell Core.
- Você pode criar e executar programas com qualquer um dos SDKs da AWS disponíveis usando as APIs de marcação de grupos de recursos, como as APIs de atribuição de tags para Python ou as APIs de atribuição de tags para Java.

Ao adicionar, remover ou editar tags existentes, você está alterando apenas as tags nos recursos que você selecionar nos resultados de sua consulta Encontrar recursos para marcar. Você pode selecionar até 500 recursos nos quais gerenciar tags.

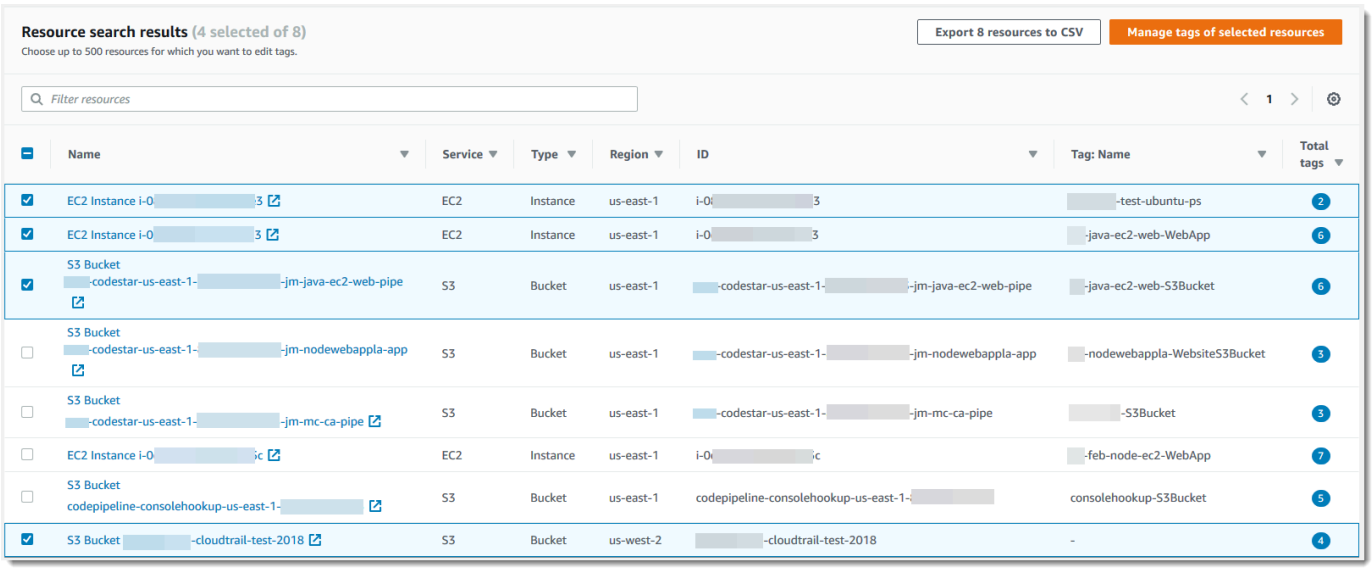
Tópicos

Adicionar tags a recursos selecionados

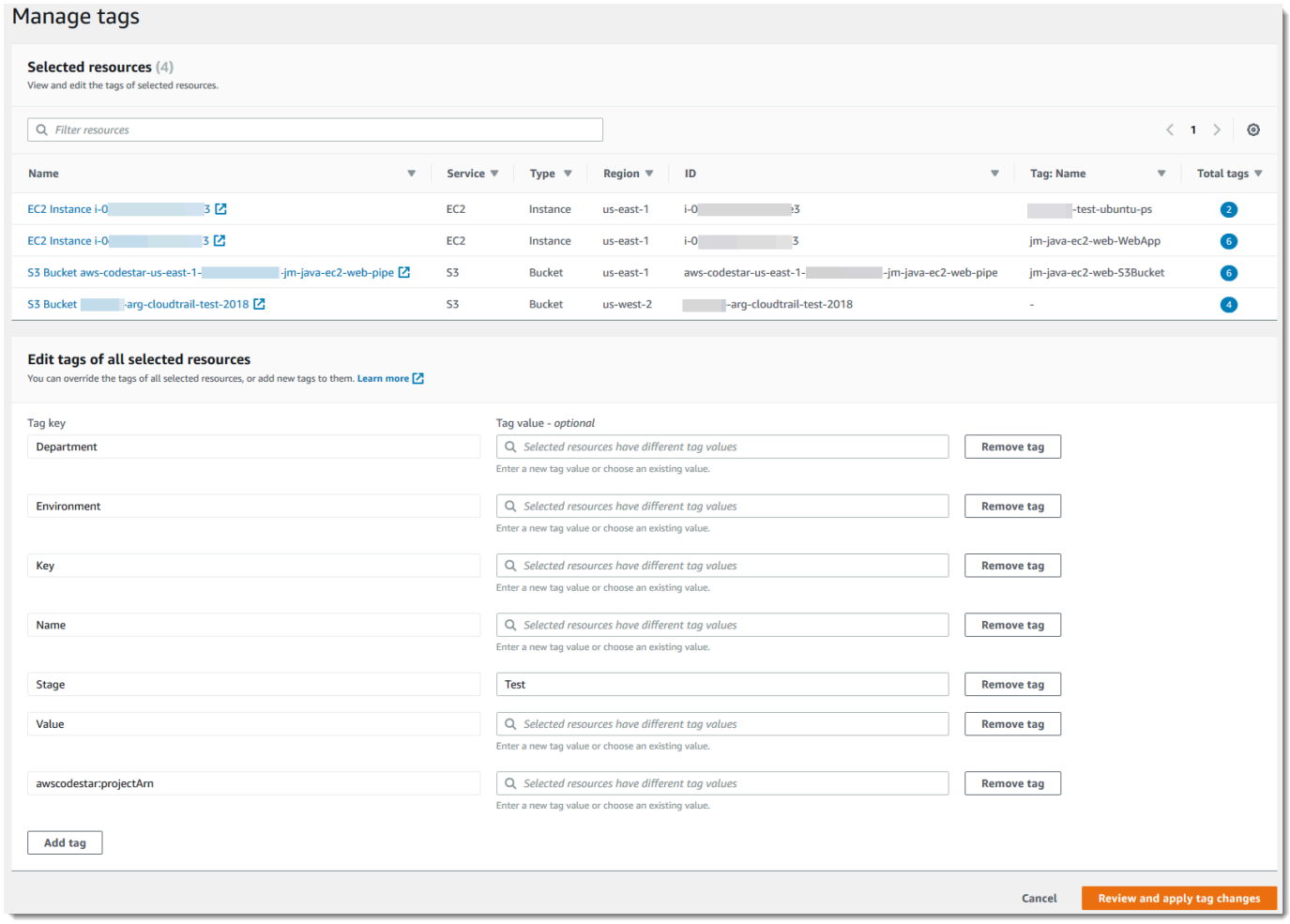
Você pode usar o Tag Editor para adicionar tags a recursos selecionados que estão nos resultados de sua consulta Encontrar recursos para marcar.

> **Note**
>
> Este tópico descreve como editar em massa as tags para vários recursos. Você também pode editar os valores de tag para um recurso individual. Para ter mais informações, consulte Exibir e editar tags para um recurso selecionado.

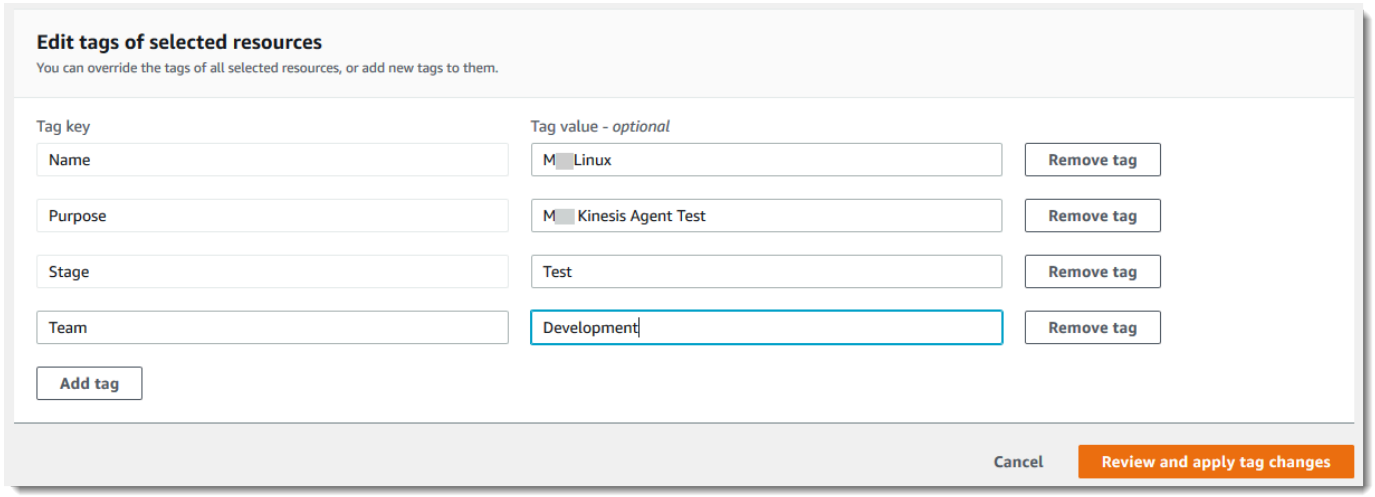
1. Abra o console do Tag Editor e envie uma consulta que retorne vários recursos que você deseja marcar.
2. Nos resultados da consulta Encontrar recursos para marcar, marque as caixas de seleção ao lado dos recursos aos quais você deseja adicionar tags. Insira uma string de texto em Filtrar recursos para filtrar por parte de um nome de recurso, ID, chaves de tags ou valores de tags. Na coluna Tags, observe que os recursos nos resultados já têm tags aplicadas a eles. No exemplo a seguir, a primeira instância do EC2 na lista já tem duas tags.



3. Marque a caixa de seleção de um ou mais recursos e depois escolha Gerenciar tags dos recursos selecionados.
4. Na página Gerenciar tags, mostrada abaixo, visualize as tags nos recursos selecionados. Embora a consulta original tenha retornado mais recursos, você está adicionando tags apenas aos recursos que selecionou na etapa 1. Escolha Adicionar Tag.



5. Insira uma chave de tag e um valor de tag opcional. Para esse procedimento, você adicionará a chave de tag **`Team`** e o valor de tag **`Development`**.



> **Note**
>
> Um recurso pode ter no máximo 50 tags aplicadas pelo usuário. Talvez você não consiga adicionar novas tags a um recurso se estiver se aproximando de 50 tags aplicadas pelo usuário. As tags geradas pela AWS não se aplicam ao limite de 50 tags. As chaves de tags também devem ser exclusivas em seus recursos selecionados. Você não pode adicionar uma nova tag com uma chave que corresponde a uma chave de tag já existente nos recursos selecionados.

6. Ao concluir a adição de tags, escolha Revisar e aplicar alterações.
7. Se você aceitar as alterações, escolha Aplicar alterações a todos os selecionados.
8. Dependendo do número de recursos que selecionar, a aplicação de novas tags pode demorar alguns minutos. Não saia da página nem abra outra página na mesma guia do navegador. Se as alterações foram bem-sucedidas, um banner de sucesso verde será exibido na parte superior da página. Aguarde até que um banner de sucesso ou de falha apareça na página para continuar.

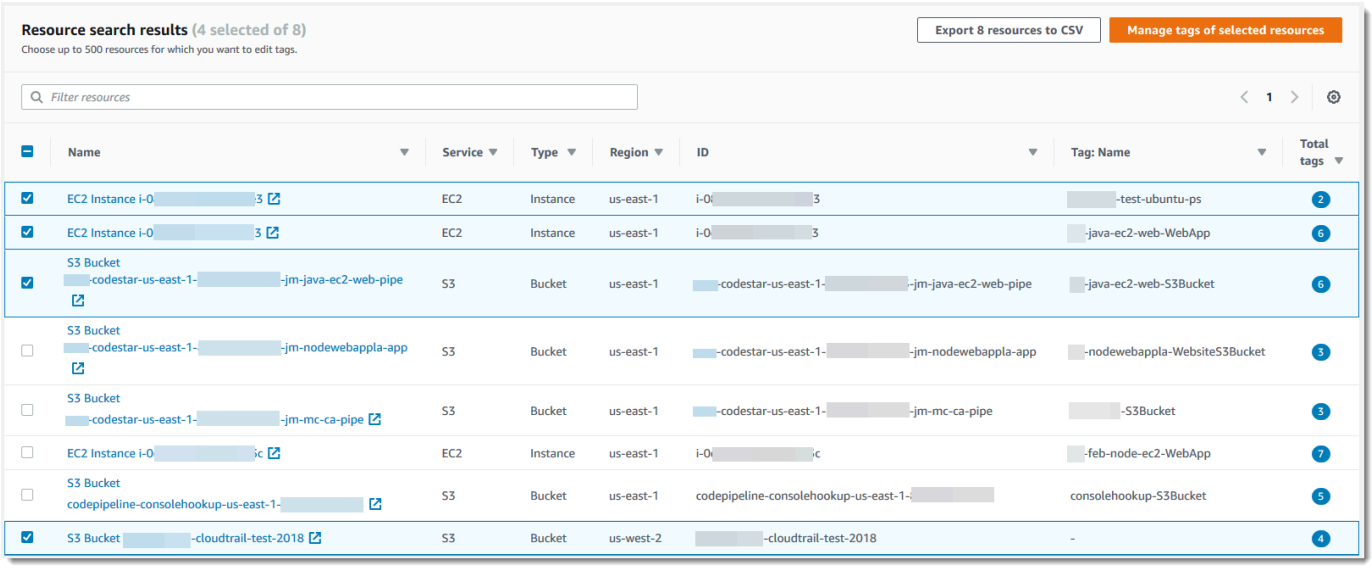
   Se as alterações de tags em alguns ou todos os recursos não forem bem-sucedidas, consulte Solução de problemas de alterações de tags. Depois de resolver as alterações de tags malsucedidas (como permissões insuficientes), você pode repetir as alterações de tags nos recursos para os quais as alterações de tags falharam. Para ter mais informações, consulte the section called “Tentar novamente as alterações de tags com falha”.

Editar tags de recursos selecionados

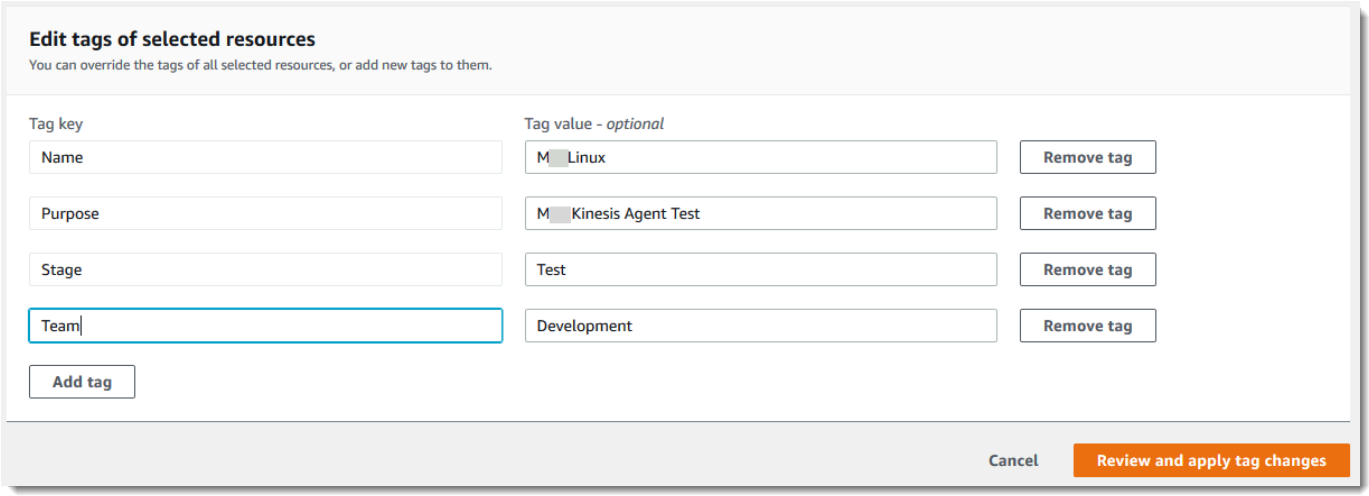
Você pode usar o Tag Editor para alterar valores de tags existentes em recursos selecionados que estão nos resultados de sua consulta Find resources to tag (Encontrar recursos para marcar). A edição de uma tag altera o valor da tag em todos os recursos selecionados que têm a mesma chave de tag. Você não pode renomear uma chave de tag, mas pode excluir uma tag e criar uma tag com um novo nome para substituir uma chave de tag original. Isso exclui todas as tags com essa chave em recursos selecionados.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. Usamos tags para fornecer serviços de cobrança e administração. As tags não devem ser usadas para dados privados ou confidenciais.

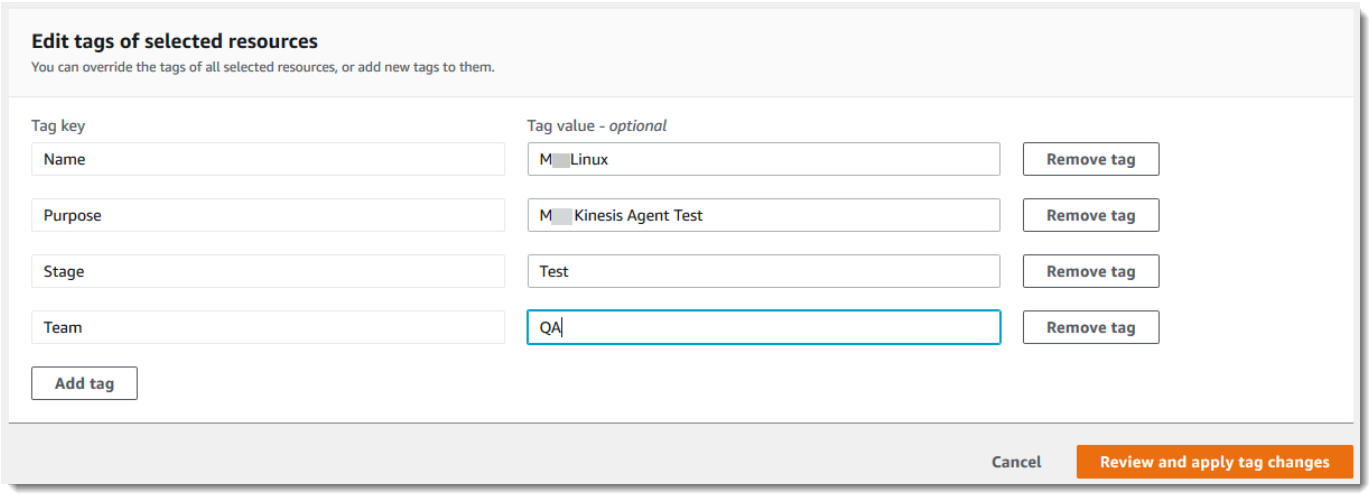
1. Nos resultados da consulta Encontrar recursos para marcar, marque as caixas de seleção ao lado dos recursos para os quais você deseja alterar tags existentes. Insira uma string de texto em Filtrar recursos para filtrar por parte de um nome ou de um ID de recurso. Na coluna Tags, observe que os recursos nos resultados já têm tags aplicadas a eles. No exemplo a seguir, a primeira instância do EC2 selecionada já tem duas tags.



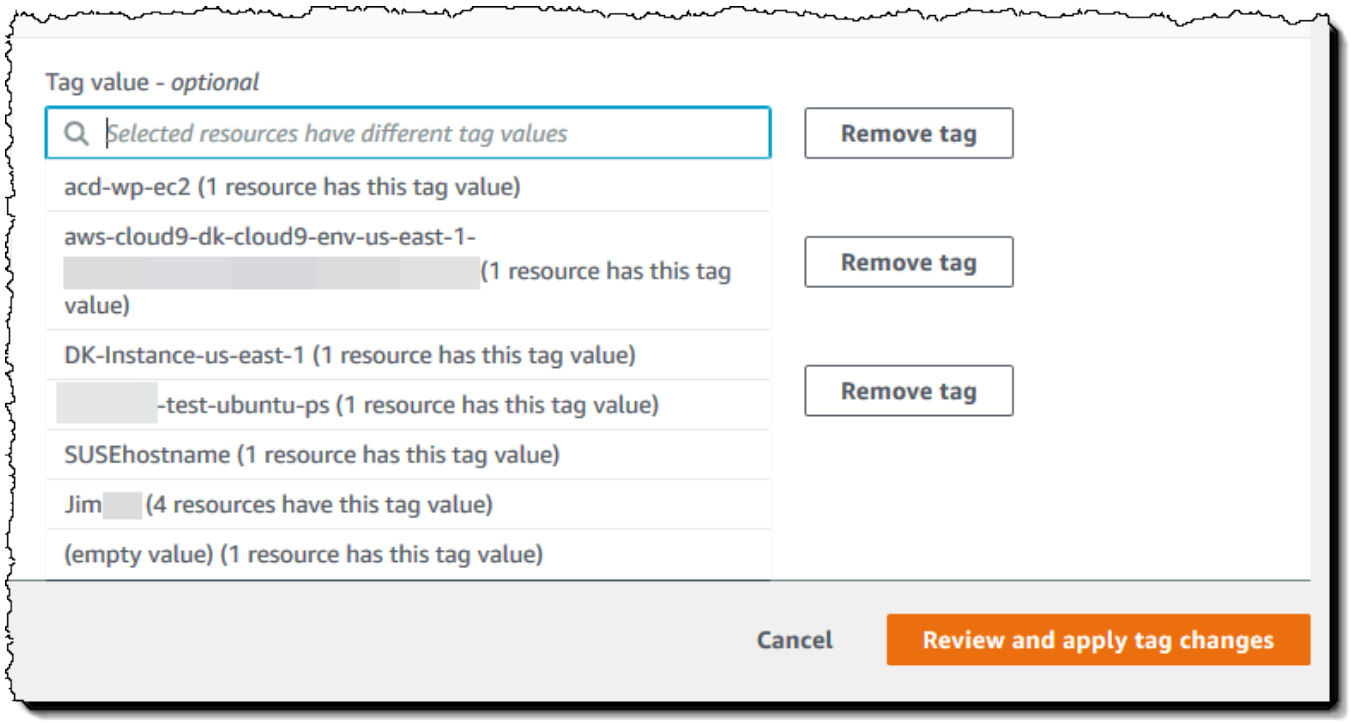
2. Escolha Gerenciar tags dos recursos selecionados.
3. Na página Gerenciar tags, em Editar tags de recursos selecionados, visualize as tags no recurso que você selecionou. Embora a consulta original possa ter retornado mais recursos, você está alterando tags apenas nos recursos que você selecionou na etapa 1.



4. Altere, adicione ou exclua os valores de tags. As tags devem ter uma chave de tag, mas os valores de tag são opcionais. Neste procedimento, alteramos o valor da tag **`Team`** para **`QA`**.

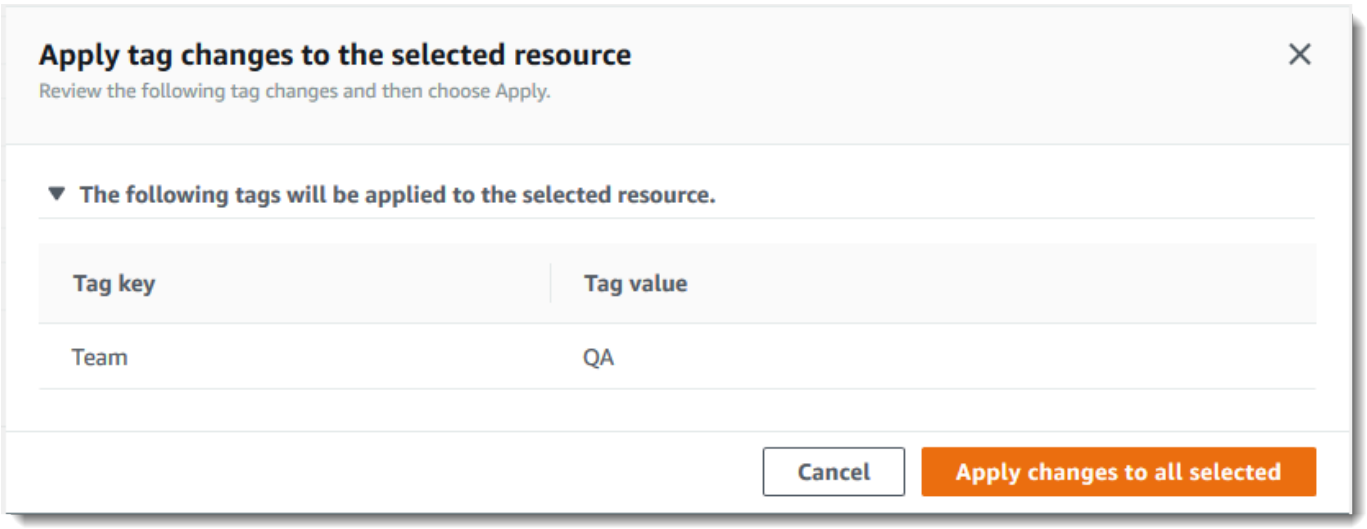


Se os recursos em sua seleção tiverem valores diferentes para a mesma chave, Recursos selecionados têm diferentes valores de tag será exibido no campo Valor da tag. Neste caso, colocar o cursor na caixa abre uma lista suspensa de todos os valores disponíveis para essa chave de tag nos recursos selecionados.



Se os recursos em sua seleção tiverem o valor da tag que você deseja, o valor da tag será realçado conforme você o digitar. Por exemplo, se os recursos em sua seleção já tiverem o valor da tag **`QA`**, o valor será realçado conforme você digitar **`Q`**. Os valores na lista suspensa ajudam a manter os valores de tag consistentes entre recursos. O valor da tag é alterado em todos os recursos selecionados. Neste exemplo, o valor da tag é alterado para **`QA`** para todos os recursos selecionados que tinham uma chave de tag **`Team`**. Para recursos selecionados que não têm a tag **`Team`**, a tag **`Team`** com o valor **`QA`** é adicionada.

5. Depois de concluir a alteração de tags, escolha Revisar e aplicar as alterações.
6. Se você aceitar as alterações, escolha Aplicar alterações a todos os selecionados.



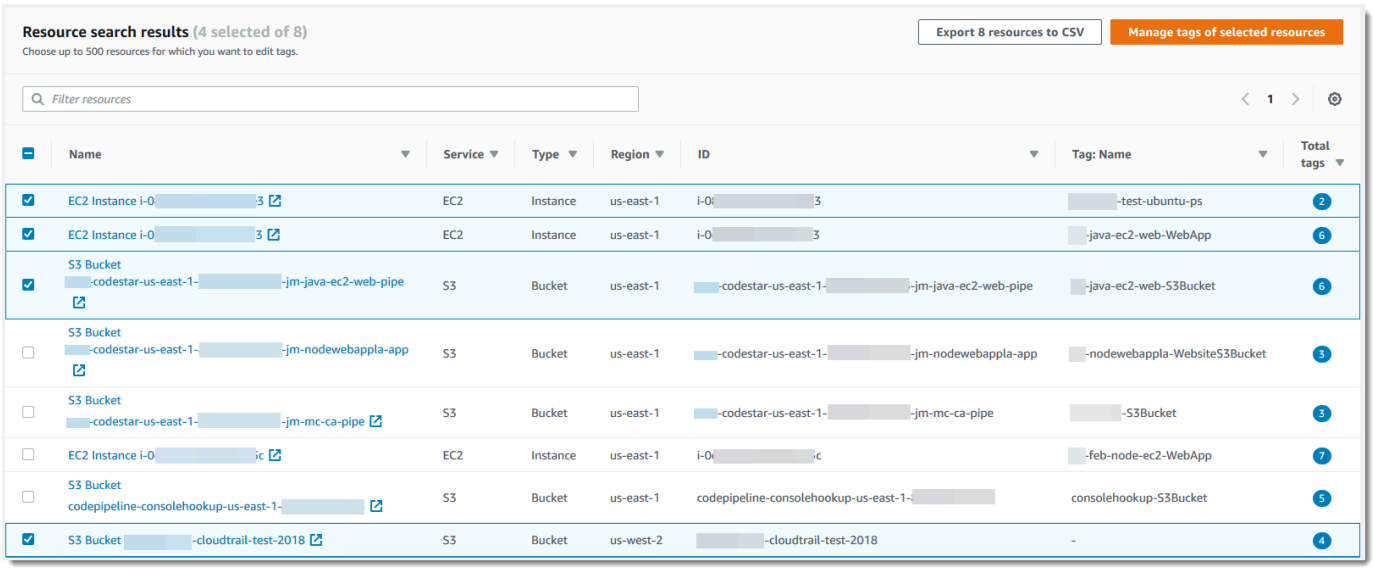
7. Dependendo do número de recursos selecionados, a edição das tags pode demorar alguns minutos. Não saia da página nem abra outra página na mesma guia do navegador. Se as alterações foram bem-sucedidas, um banner de sucesso verde será exibido na parte superior da página. Aguarde até que um banner de sucesso ou de falha apareça na página para continuar.

   Se as alterações de tags em alguns ou todos os recursos não forem bem-sucedidas, consulte Solução de problemas de alterações de tags. Depois de resolver as causas raiz de alterações de tags malsucedidas (como permissões insuficientes), você pode repetir as alterações de tags nos recursos para os quais as alterações de tags falharam. Para ter mais informações, consulte the section called “Tentar novamente as alterações de tags com falha”.

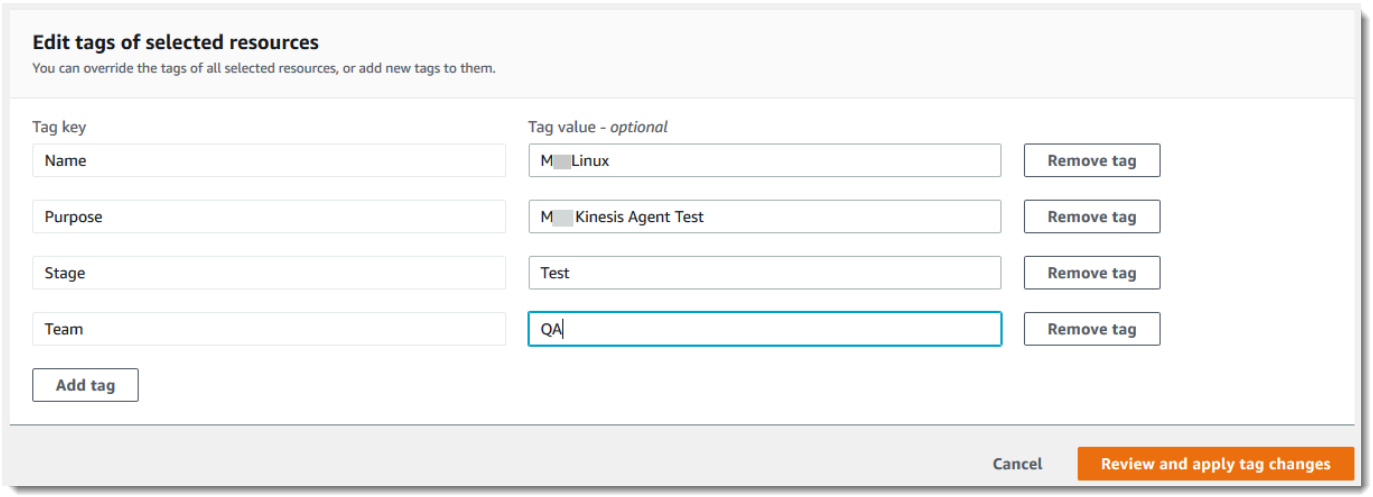
Remover tags de recursos selecionados

Você pode usar o Tag Editor para remover tags de recursos selecionados que estão nos resultados da consulta Encontrar recursos para marcar. A remoção de uma tag exclui a tag de todos os recursos selecionados que têm a tag. Como você não pode editar chaves de tags, você pode remover tags e substituí-las por novas tags se for necessário editar uma chave de tag. Isso exclui todas as tags com essa chave em recursos selecionados.

1. Nos resultados da consulta Encontrar recursos para marcar, marque as caixas de seleção ao lado dos recursos dos quais você deseja remover tags. Insira uma string de texto em Filtrar recursos para filtrar por parte de um nome ou de um ID de recurso.

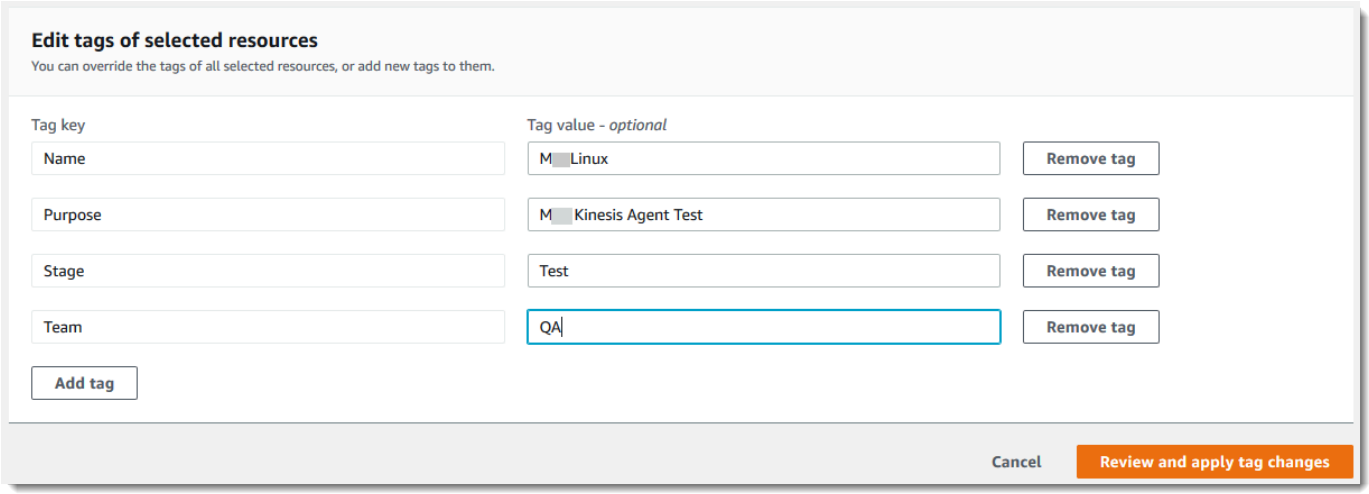


2. Escolha Gerenciar tags dos recursos selecionados.
3. Na página Gerenciar tags, em Editar tags dos recursos selecionados, visualize as tags nos recursos selecionados. Embora a consulta original possa ter retornado mais recursos, você está alterando tags apenas nos recursos que você selecionou na etapa 1.



4. Escolha Remover tag ao lado de qualquer tag que você deseja excluir. Neste procedimento, removemos a tag **`Team`**.

> **Note**
>
> A escolha de Remover tag remove uma tag de todos os recursos selecionados que têm a tag. No exemplo mostrado, isso remove a tag **`Team`** de todos os recursos selecionados que tiverem a tag **`Team`**, independentemente do valor da tag.



5. Escolha Revisar e aplicar alterações.
6. Na página de confirmação, escolha Aplicar alterações a todos os selecionados.
7. Dependendo do número de recursos selecionados, a remoção de tags pode demorar alguns minutos. Não saia da página nem abra outra página na mesma guia do navegador. Se as alterações foram bem-sucedidas, um banner de sucesso verde será exibido na parte superior da página. Aguarde até que um banner de sucesso ou de falha apareça na página para continuar.

   Se as alterações de tags em alguns ou todos os recursos não forem bem-sucedidas, consulte Solução de problemas de alterações de tags. Depois de resolver as causas raiz de alterações de tags malsucedidas (como permissões insuficientes), você pode repetir as alterações de tags nos recursos para os quais as alterações de tags falharam. Para ter mais informações, consulte the section called “Tentar novamente as alterações de tags com falha”.

Tentar novamente as alterações de tags com falha

Se as alterações de tag falharem em pelo menos um dos recursos selecionados, o Tag Editor exibirá um banner vermelho na parte inferior da página. O banner mostra mensagens de erro para cada tipo de falha que ocorre. Para cada erro, o banner identifica os recursos específicos em que o Tag Editor não pôde fazer alterações de tag. Após revisar e solucionar os erros, escolha Tentar novamente as alterações de tags com falha em recursos para repetir as alterações somente nesses recursos em que as alterações de tag falharam.

Informações relacionadas

- Usar tags de alocação de custos no Guia do usuário do AWS Billing

Como usar tags nas políticas de permissão do IAM

AWS Identity and Access Management (IAM) é o AWS service (Serviço da AWS) que você usa para criar e gerenciar políticas de permissões que determinam quem pode acessar seus recursos da AWS. Toda tentativa de acessar um serviço da AWS ou ler ou gravar um recurso da AWS é controlada por uma política do IAM.

Essas políticas permitem que você forneça acesso detalhado aos seus recursos. Um dos recursos que você pode usar para ajustar esse acesso é o elemento de `Condition` da política. Esse elemento permite especificar as condições que devem corresponder à solicitação para determinar se a solicitação pode continuar. Entre as coisas que você pode verificar com o elemento de `Condition` estão as seguintes:

- Tags que são anexadas ao usuário ou perfil que faz a solicitação.
- Tags anexadas ao recurso que é o objeto da solicitação.

Chaves de condição relacionadas às tags

A tabela a seguir descreve as chaves de condição que podem ser usadas em uma política de permissões do IAM para controlar o acesso com base em tags. Essas chaves de condição permitem que você faça o seguinte:

- Compare as tags da entidade principal que está chamando a operação.
- Compare as tags fornecidas para a operação como um parâmetro.
- Compare as tags anexadas ao recurso que seria acessado pela operação.

Para obter detalhes completos sobre uma chave de condição e como usá-la, consulte a página com link na coluna Nome da chave de condição.

Nome da chave de condição	Descrição
aws:PrincipalTag	Compara a tag anexada à entidade principal (usuário ou perfil do IAM) ou que está fazendo a solicitação com a tag especificada na política.
aws:RequestTag	Compara o par valor-chave da tag que foi passado para a solicitação como parâmetro com o par valor-chave da tag que você especificar na política.
aws:ResourceTag	Compara o par valor-chave que é anexado ao recurso com o par valor-chave que você especificar na política.
aws:TagKeys	Compara somente chaves de tag na solicitação com as chaves que você especificar na política.

Exemplos de políticas do IAM que usam tags

Example Exemplo 1: forçar os usuários a anexar uma tag específica ao criar um recurso

O exemplo a seguir da política de permissões do IAM mostra como forçar o usuário que cria ou modifica as tags de uma política do IAM para incluir uma tag com a chave do `Owner`. Além disso, a política exige que o valor da tag seja definido com o mesmo valor da tag do `Owner` atualmente anexada à entidade principal da chamada. Para que essa estratégia funcione, todas as entidades principais devem ter uma tag do `Owner` anexada e os usuários devem ser impedidos de modificar essa tag. Se ocorrer uma tentativa de criar ou modificar uma política sem incluir a tag do `Owner`, a política não corresponderá e a operação não será permitida.

```
{
    "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 Exemplo 2: usar tags para limitar o acesso a um recurso para seu “proprietário”

O exemplo de política de permissões do IAM permite que o usuário interrompa uma instância do Amazon EC2 em execução somente se a entidade principal da chamada estiver marcada com o mesmo valor de tag do `project` que a instância.

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

Este é um exemplo de controle de acesso por atributo (ABAC). Para obter mais informações e exemplos adicionais do uso de políticas do IAM para implementar uma estratégia de controle de acesso baseada em tags, consulte os tópicos a seguir no Guia do usuário do AWS Identity and Access Management:

- Controlar o acesso a recursos da AWS usando tags
- Controlar acesso para usuários e perfis do IAM usando tags
- Tutorial do IAM: definir permissões para acessar recursos da AWS com base em tags; mostra como conceder acesso a diferentes projetos e grupos usando várias tags.

Políticas de tag do AWS Organizations

Uma política de tag é um tipo de política que você cria no AWS Organizations. Você pode usar políticas de tag para ajudar a padronizar tags nos recursos das contas da sua organização. Para usar políticas de tag, recomendamos que você siga os fluxos de trabalho descritos em Conceitos básicos das políticas de tag no Guia do usuário do AWS Organizations. Conforme mencionado nessa página, os fluxos de trabalho recomendados incluem encontrar e corrigir tags não compatíveis. Para executar essas tarefas, você utiliza o console do Tag Editor.

Tópicos

Pré-requisitos e permissões

Antes de avaliar a conformidade com as políticas de tag no Tag Editor, você deve atender aos requisitos e definir as permissões necessárias.

Pré-requisitos para avaliar a conformidade com as políticas de tag

A avaliação da compatibilidade com políticas de tag requer o seguinte:

- Primeiro, você deve habilitar o atributo no AWS Organizations e criar e anexar políticas de tag. Para obter mais informações, consulte as seguintes páginas do Guia do usuário do AWS Organizations:
  - Pré-requisitos e permissões para gerenciar políticas de tag
  - Habilitar políticas de tag
  - Conceitos básicos das políticas de tag
- Para encontrar tags não compatíveis nos recursos de uma conta, você precisa das credenciais de login dessa conta e das permissões listadas em Permissões para avaliar a conformidade de uma conta.
- Para avaliar a conformidade em toda a organização, você precisa das credenciais de login da conta de gerenciamento da organização e das permissões listadas em Permissões para avaliar a conformidade em toda a organização . Você pode solicitar o relatório de conformidade somente para a Região da AWS Leste dos EUA (Norte da Virgínia).

Permissões para avaliar a conformidade de uma conta

Encontrar tags não compatíveis nos recursos de uma conta requer as seguintes permissões:

- `organizations:DescribeEffectivePolicy`: para obter o conteúdo da política de tag efetiva para a conta.
- `tag:GetResources`: para obter uma lista de recursos que não estão em conformidade com a política de tag anexada.
- `tag:TagResources`: para adicionar ou atualizar tags. Você também precisa de permissões específicas do serviço para criar tags. Por exemplo, para atribuir tags em recursos no Amazon Elastic Compute Cloud (Amazon EC2), você precisa ter permissões para `ec2:CreateTags`.
- `tag:UnTagResources`: para remover uma tag. Você também precisa de permissões específicas do serviço para remover as tags. Por exemplo, para remover a tag de recursos no Amazon EC2, você precisa ter permissões para `ec2:DeleteTags`.

O exemplo de política de AWS Identity and Access Management (IAM) a seguir fornece permissões para avaliar a conformidade de tags de uma conta.

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

Para obter mais informações sobre as políticas e as permissões do IAM, consulte o Guia do usuário do IAM.

Permissões para avaliar a conformidade em toda a organização

A avaliação da conformidade em toda a organização com as políticas de tag requer as seguintes permissões:

- `organizations:DescribeEffectivePolicy`: para obter o conteúdo da política de tag que está anexada à organização, unidade organizacional (UO) ou conta.
- `tag:GetComplianceSummary`: para obter um resumo dos recursos não compatíveis em todas as contas da organização.
- `tag:StartReportCreation`: para exportar os resultados da avaliação de conformidade mais recente para um arquivo. A conformidade em toda a organização é avaliada a cada 48 horas.
- `tag:DescribeReportCreation`: para verificar o status de criação do relatório.

O exemplo de política do IAM a seguir fornece permissões para avaliar a conformidade em toda a organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateOrgCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetComplianceSummary",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre as políticas e as permissões do IAM, consulte o Guia do usuário do IAM.

Política de bucket do Amazon S3 para armazenamento de relatórios

Para criar um relatório de conformidade para toda a organização, é necessário conceder acesso à entidade principal do serviço de políticas de tag a um bucket do Amazon Simple Storage Service

(Amazon S3) na região Leste dos EUA (Norte da Virgínia) para armazenamento de relatórios. Anexe a seguinte política de bucket ao bucket, substituindo cada *espaço reservado* por suas próprias informações:

- Nome de seu bucket do S3
- Número de ID da organização
- Número de ID da conta de gerenciamento da organização para a organização na qual você está aplicando a política

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "tagpolicies.tag.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<your-bucket-name>",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": "<organization-management-account-id>",
                    "aws:SourceArn": "arn:aws:tag:us-east-1:<organization-management-
account-id>:*"
                }
            }
        },
        {
            "Sid": "TagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "tagpolicies.tag.amazonaws.com"
                ]
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
```

```
            ],
            "Resource": "arn:aws:s3:::<your-bucket-name>/AwsTagPolicies/<your-
organization-id>/*",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": "<organization-management-account-id>",
                    "aws:SourceArn": "arn:aws:tag:us-east-1:<organization-management-
account-id>:*"
                }
            }
        }
    ]
}
```

Avaliação da conformidade de uma conta

Você pode avaliar a conformidade de uma conta em sua organização com sua política de tag efetiva.

> **Important**
>
> Os recursos sem tag não são exibidos como incompatíveis nos resultados.
> Para encontrar recursos sem tag em sua conta, use Explorador de recursos da AWS com uma consulta que use **`tag:none`**. Para obter mais informações, consulte Pesquisa de recursos sem tags no Guia do usuário do Explorador de recursos da AWS.

A política de tags efetiva especifica as regras de atribuição de tags que se aplicam a uma conta. A política de tag efetiva é a agregação de todas as políticas de tag que a conta herda, além de qualquer política de tag diretamente anexada à conta. Quando você anexa uma política de tags à raiz da organização, ela se aplica a todas as contas na organização. Quando você anexa uma política de tag a uma unidade organizacional (UO), ela se aplica a todas as contas e UOs que pertencem à UO.

> **Note**
>
> Se você ainda não criou políticas de tag, consulte Conceitos básicos das políticas de tag no Guia do usuário do AWS Organizations.

Para encontrar tags não compatíveis, você precisa ter as seguintes permissões:

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

Para avaliar a conformidade de uma conta com sua política de tag efetiva (console)

1. Enquanto estiver conectado à conta cuja conformidade você deseja verificar, abra o Console de políticas de tag.
2. A seção Política de tag efetiva mostra quando a política foi atualizada pela última vez e as chaves de tag definidas. Você pode expandir uma chave de tag para ver informações sobre seus valores, tratamento de caso e se os valores são aplicados para tipos de recursos específicos.

   > **Note**
   >
   > Se você estiver conectado à conta de gerenciamento, precisará escolher uma conta para ver sua política efetiva e visualizar as informações de conformidade.

3. Na seção Recursos com tags não compatíveis, especifique qual Região da AWS pesquisar por tags não compatíveis. Se preferir, você também poderá pesquisar por tipo de recurso. Em seguida, escolha Recursos de pesquisa.

   Os resultados em tempo real são mostrados na seção Resultados da pesquisa. Para alterar o número de resultados retornados por página ou as colunas a serem exibidas, escolha o ícone de configurações ().
4. Nos resultados da pesquisa, selecione um recurso com tags não compatíveis.
5. Na caixa de diálogo que lista as tags do recurso, escolha o link para abrir o AWS service (Serviço da AWS) onde o recurso foi criado. Nesse console, corrija a tag não compatível.

> **Tip**
>
> Se você não tiver certeza de quais tags não são compatíveis, acesse a seção Política de tag efetiva da conta no console de políticas de tag. Você pode expandir uma chave de tag para ver suas regras de marcação.

6. Repita o processo de encontrar e corrigir tags até que os recursos da conta que lhe interessam estejam em conformidade em cada região.

Para encontrar tags não compatíveis (AWS CLI, API da AWS)

Use os comandos e operações a seguir para encontrar tags não compatíveis:

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

  Para obter o procedimento completo de uso de políticas de tag no AWS CLI, consulte Usar políticas de tag no AWS CLI no Guia do usuário do AWS Organizations.
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Próximas etapas

Recomendamos que você repita o processo de encontrar e corrigir problemas de conformidade. Continue até que os recursos com os quais você se preocupa estejam compatíveis com a política de tag efetiva em cada região.

Encontrar e corrigir tags não compatíveis é um processo iterativo por vários motivos, incluindo os seguintes:

- O uso das políticas de tag pela sua organização pode evoluir com o tempo.
- Leva tempo para efetuar mudanças em sua organização ao criar recursos.

- A conformidade pode mudar sempre que um novo recurso é criado ou quando novas tags são atribuídas a um recurso.
- A política de tag efetiva de uma conta é atualizada sempre que uma política de tag é anexada ou separada dela. A política de tag efetiva também é atualizada sempre que ocorrem alterações nas políticas que a conta herda.

Se estiver conectado como a conta de gerenciamento da organização, você também poderá gerar um relatório. Esse relatório mostra informações sobre todos os recursos marcados das contas de sua organização. Para ter mais informações, consulte Avaliar a conformidade em toda a organização.

Avaliar a conformidade em toda a organização

Você pode avaliar a conformidade da sua organização com a política de tag efetiva. Você pode gerar um relatório que liste todos os recursos marcados em contas em toda a organização e que indique se cada recurso está em conformidade com a política de tag em vigor.

> **Important**
>
> Os recursos sem tag não são exibidos como incompatíveis nos resultados.
> Para encontrar recursos sem tag em sua conta, use Explorador de recursos da AWS com uma consulta que use **`tag:none`**. Para obter mais informações, consulte Pesquisa de recursos sem tags no Guia do usuário do Explorador de recursos da AWS.

Você pode gerar o relatório a partir da conta de gerenciamento da organização apenas na Região da AWS `us-east-1`. A conta que gera o relatório deve ter acesso a um bucket do Amazon S3 na região Leste dos EUA (Norte da Virgínia). O bucket deve ter uma política de bucket anexada, conforme mostrado em Política de bucket do Amazon S3 para relatório de armazenamento.

Para gerar um relatório de compatibilidade com toda a organização, você deve ter as seguintes permissões:

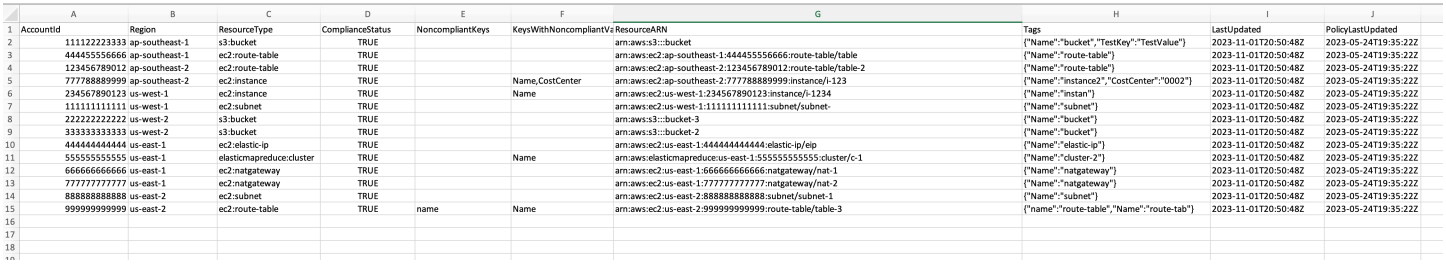
- `organizations:DescribeEffectivePolicy`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `tag:GetComplianceSummary`

Para gerar um relatório de conformidade em toda a organização (console)

1. Abra o Console de políticas de tag.
2. Escolha a guia Raiz desta organização e, na parte inferior da página, escolha Gerar relatório.
3. Na tela Gerar relatório, especifique onde armazenar o relatório.
4. Escolha Iniciar exportação.

Quando o relatório estiver concluído, você poderá baixá-lo na seção Relatório de não conformidade na guia Raiz da organização.

Veja a seguir um exemplo de trecho do relatório.



	A	B	C	D	E	F	G	H	I	J
1	AccountId	Region	ResourceType	ComplianceStatus	NoncompliantKeys	KeysWithNoncompliantVa	ResourceARN	Tags	LastUpdated	PolicyLastUpdated
2	111122223333	ap-southeast-1	s3:bucket	TRUE			arn:aws:s3:::bucket	{"Name":"bucket","TestKey":"TestValue"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
3	444455556666	ap-southeast-1	ec2:route-table	TRUE			arn:aws:ec2:ap-southeast-1:444455556666:route-table/table	{"Name":"route-table"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
4	123456789012	ap-southeast-2	ec2:route-table	TRUE			arn:aws:ec2:ap-southeast-2:123456789012:route-table/table-2	{"Name":"route-table"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
5	777788889999	ap-southeast-2	ec2:instance	TRUE		Name,CostCenter	arn:aws:ec2:ap-southeast-2:777788889999:instance/i-123	{"Name":"instance2","CostCenter":"0002"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
6	234567890123	us-west-1	ec2:instance	TRUE		Name	arn:aws:ec2:us-west-1:234567890123:instance/i-1234	{"Name":"instan"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
7	111111111111	us-west-1	ec2:subnet	TRUE			arn:aws:ec2:us-west-1:111111111111:subnet/subnet-	{"Name":"subnet"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
8	222222222222	us-west-2	s3:bucket	TRUE			arn:aws:s3:::bucket-3	{"Name":"bucket"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
9	333333333333	us-west-2	s3:bucket	TRUE			arn:aws:s3:::bucket-2	{"Name":"bucket"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
10	444444444444	us-east-1	ec2:elastic-ip	TRUE			arn:aws:ec2:us-east-1:444444444444:elastic-ip/eip	{"Name":"elastic-ip"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
11	555555555555	us-east-1	elasticmapreduce:cluster	TRUE		Name	arn:aws:elasticmapreduce:us-east-1:555555555555:cluster/c-1	{"Name":"cluster-2"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
12	666666666666	us-east-1	ec2:natgateway	TRUE			arn:aws:ec2:us-east-1:666666666666:natgateway/nat-1	{"Name":"natgateway"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
13	777777777777	us-east-1	ec2:natgateway	TRUE			arn:aws:ec2:us-east-1:777777777777:natgateway/nat-2	{"Name":"natgateway"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
14	888888888888	us-east-2	ec2:subnet	TRUE			arn:aws:ec2:us-east-2:888888888888:subnet/subnet-1	{"Name":"subnet"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
15	999999999999	us-east-2	ec2:route-table	TRUE	name	Name	arn:aws:ec2:us-east-2:999999999999:route-table/table-3	{"name":"route-table","Name":"route-tab"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
16										
17										
18										

Observações

A conformidade em toda a organização é avaliada a cada 48 horas. Isso resulta no seguinte:

- Observe que pode levar até 48 horas para que as alterações em uma política de tag ou recursos sejam refletidas no relatório de conformidade em toda a organização. Por exemplo, suponha que você tenha uma política de tag que define uma nova tag padronizada para um tipo de recurso. Os recursos desse tipo que não têm essa tag podem ser mostrados como compatíveis no relatório por até 48 horas.
- Embora você possa gerar o relatório a qualquer momento, os resultados do relatório não são atualizados até que a próxima avaliação seja concluída.
- A NoncompliantKeyscoluna lista as chaves de tag no recurso que não estão em conformidade com a política de tags efetiva.
- A KeysWithNonCompliantValuescoluna lista as chaves definidas na política efetiva que estão no recurso com tratamento de caso incorreto ou valores não compatíveis.
- Se você fechar uma Conta da AWS que era membro da organização, ela poderá continuar aparecendo no relatório de conformidade da tag por até 90 dias.

Para gerar um relatório de conformidade em toda a organização (AWS CLI, API da AWS)

Use os comandos e as operações a seguir para gerar um relatório de conformidade em toda a organização, verificar seu status e visualizar o relatório:

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

  Para obter o procedimento completo de uso de políticas de tag no AWS CLI, consulte Usar políticas de tag no AWS CLI no Guia do usuário do AWS Organizations.
- API da AWS:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

Monitore as alterações de tags com fluxos de trabalho sem servidor e a Amazon EventBridge

A Amazon EventBridge suporta alterações de tags em AWS recursos. Usando esse EventBridge tipo, você pode criar EventBridge regras para corresponder às alterações de tag e rotear os eventos para um ou mais destinos. Por exemplo, um destino pode ser uma função AWS Lambda para invocar fluxos de trabalho automatizados. Este tópico fornece um tutorial sobre como usar o Lambda para criar uma solução econômica com tecnologia sem servidor para processar com segurança as alterações de tags em seus recursos da AWS.

Alterações de tag geram EventBridge eventos

EventBridge fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. Muitos recursos da AWS oferecem suporte a tags, que são atributos personalizados definidos pelo usuário para organizar e categorizar os recursos da AWS com facilidade. Os casos de uso comuns de tags são categorização de alocação de custos, segurança de controle de acesso e automação.

Com EventBridge, você pode monitorar as alterações nas tags e rastrear o estado das tags nos AWS recursos. Anteriormente, para obter uma funcionalidade semelhante, você poderia ter pesquisado continuamente as APIs e orquestrado várias chamadas. Agora, qualquer alteração em uma tag, incluindo APIs de serviços individuais, o Tag Editor e a API de marcação, iniciará a alteração de tag no evento do recurso. O exemplo a seguir mostra um EventBridge evento típico solicitado por uma alteração de tag. Ele mostra as chaves de tags novas, atualizadas ou excluídas e seus valores associados.

```
{
  "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,
  }
}
```

Todos os EventBridge eventos têm os mesmos campos de nível superior:

- versão: por padrão, este valor é definido como `0` (zero) em todos os eventos.
- id: um valor exclusivo é gerado para cada evento. Isso pode ser útil em eventos de rastreamento ao percorrerem regras e destinos e serem processados.

- tipo de detalhe: identifica, em combinação com o campo `source`, os campos e os valores que serão exibidos no campo de detalhes.
- origem: identifica o serviço que foi a origem do evento. A origem das alterações de tags é `aws.tag`.
- hora: a hora do evento.
- região: identifica a Região da AWS onde o evento foi originado.
- recursos: essa matriz JSON contém os nomes dos recursos da Amazon (ARN) que identificam os recursos que estão envolvidos no evento. Esse é o recurso em que as tags foram alteradas.
- detalhe: um objeto JSON cujo conteúdo é diferente dependendo do tipo de evento. Para alteração de tag no recurso, os seguintes campos detalhados estão incluídos:
  - changed-tag-keys— As chaves de tag que foram alteradas por esse evento.
  - serviço: o serviço ao qual o recurso pertence. Neste exemplo, o serviço é `ec2`, que é o Amazon EC2.
  - tipo de recurso: o tipo de recurso do serviço. Neste exemplo, é uma instância do Amazon EC2.
  - versão: a versão do conjunto de tags. A versão começa em 1 e aumenta quando as tags são alteradas. Você pode usar a versão para verificar a ordem dos eventos de alteração de tags.
  - tags: as tags anexadas ao recurso após a alteração.

Para obter mais informações, consulte os padrões de EventBridge eventos da Amazon no Guia EventBridge do usuário da Amazon.

Ao usar EventBridge, você pode criar regras que correspondam a padrões de eventos específicos com base nos diferentes campos. Demonstramos como fazer isso no tutorial. Além disso, mostramos como uma instância do Amazon EC2 pode ser interrompida automaticamente se uma tag especificada não estiver anexada à instância. Usamos os EventBridge campos para criar um padrão que corresponda aos eventos de tag da instância que lança uma função Lambda.

Lambda e tecnologia sem servidor

O AWS Lambda segue o paradigma da tecnologia sem servidor para executar código na nuvem. Você executa o código somente quando necessário, sem pensar em servidores. Você paga apenas pelo tempo de computação que utiliza. Embora seja chamado de tecnologia sem servidor, isso não significa que não haja servidores. A tecnologia sem servidor, nesse contexto, significa que você não precisa provisionar, configurar ou gerenciar os servidores usados para executar seu código.

A AWS faz tudo isso por você, para que você possa se concentrar no seu código. Para obter mais informações sobre Lambda, consulte a Visão geral do produto do AWS Lambda.

Tutorial: interromper automaticamente as instâncias do Amazon EC2 que não têm as tags necessárias

Tópicos

À medida que seu grupo de recursos da AWS e as Contas da AWS que você gerencia crescem, você pode usar tags para facilitar a categorização de seus recursos. As tags são comumente usadas para casos de uso críticos, como alocação de custos e segurança. Para gerenciar recursos da AWS de forma eficaz, seus recursos precisam ser marcados de forma consistente. Muitas vezes, quando um recurso é provisionado, ele recebe todas as tags apropriadas. No entanto, um processo posterior pode resultar em uma alteração de tag que resulta em um desvio da política de tag corporativa. Ao monitorar as alterações em suas tags, você pode identificar um desvio de tag e responder imediatamente. Isso lhe dá mais confiança de que os processos que dependem da categorização adequada de seus recursos produzirão os resultados desejados.

O exemplo a seguir demonstra como monitorar as alterações de tags nas instâncias do Amazon EC2 para verificar se uma instância especificada continua com as tags necessárias. Se as tags da instância mudarem e a instância não tiver mais as tags necessárias, uma função do Lambda será invocada para desligar a instância automaticamente. Por que você faria isso? Isso garante que todos os recursos sejam marcados de acordo com sua política corporativa de tags, para uma alocação efetiva de custos ou para poder confiar na segurança com base no controle de acesso por atributo (ABAC).

> **Important**
>
> É altamente recomendável que você execute este tutorial em uma conta que não seja de produção, na qual não seja possível desligar inadvertidamente instâncias importantes.

O código de exemplo neste tutorial limita intencionalmente o impacto desse cenário somente às instâncias em uma lista de IDs de instância. Você deve atualizar a lista com os IDs de instância que deseja encerrar para o teste. Isso ajuda a garantir que você não consiga desligar acidentalmente todas as instâncias em uma região de sua Conta da AWS.
Após o teste, verifique se todas as suas instâncias estão marcadas de acordo com a estratégia de marcação da sua empresa. Em seguida, você pode remover o código que limita a função somente aos IDs da instância na lista.

Este exemplo usa JavaScript e a versão 16.x do Node.js. O exemplo usa o ID de exemplo 123456789012 da Conta da AWS e Região da AWS: Leste dos EUA (Norte da Virgínia) (`us-east-1`). Substitua essas informações por seu próprio ID e região da conta de teste.

Note

Se seu console usa uma região diferente como padrão, mude a região que você está usando neste tutorial sempre que mudar de console. Uma causa comum da falha desse tutorial é ter a instância e a função em duas regiões diferentes.

Se você usar uma região diferente de `us-east-1`, altere todas as referências nos exemplos de código a seguir para a região escolhida.

Etapa 1. Criar a função do Lambda

Para criar a função do Lambda

1. Abra o console de gerenciamento do AWS Lambda.
2. Selecione Criar função e Criar desde o início.
3. Em Nome da função, insira **`AutoEC2Termination`**.
4. Em Runtime, selecione Node.js 16.x.
5. Deixe todos os outros campos nos valores padrão e escolha Criar função.
6. Na guia Código da página de detalhes de `AutoEC2Termination`, abra o arquivo index.js para visualizar seu código.
   - Se uma guia com index.js abrir, você poderá escolher a caixa de edição nessa guia para editar seu código.

- Se uma guia com index.js não abrir, clique com o botão direito do mouse no arquivo index.js na pasta AutoEC2Terminator no painel de navegação. Em seguida, escolha Abrir.

7. Na guia index.js, cole o código a seguir na caixa do editor, substituindo tudo o que já estiver presente.

   Substitua o valor `RegionToMonitor` pela região na qual deseja executar essa função.

```
// 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 Conta da
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. Escolha Implantar para salvar suas alterações e ativar a nova versão da função.

Essa função Lambda verifica as tags de uma instância do Amazon EC2, conforme relatado pelo evento de alteração de tag em. EventBridge Neste exemplo, se a instância do evento não tiver a chave de tag necessária `valid-key` ou se essa tag não tiver o valor `valid-value`, a função tentará interromper a instância. Você pode alterar essa verificação lógica ou os requisitos de tag para seus próprios casos de uso específicos.

Mantenha a janela do console do Lambda aberta no navegador.

Etapa 2. Configurar as permissões necessárias do IAM

Antes que a função possa ser executada com sucesso, você deve conceder à função a permissão para interromper uma instância do EC2. O perfil fornecido da AWS lambda_basic_execution não tem essa permissão. Neste tutorial, você modifica a política de permissão padrão do IAM que está anexada ao perfil de execução da função chamada `AutoEC2Termination-role-`*`uniqueid`*. A permissão adicional mínima necessária para este tutorial é `ec2:StopInstances`.

Para obter mais informações sobre criar políticas do IAM específicas do Amazon EC2, consulte Amazon EC2: permite iniciar ou interromper uma instância do EC2 e modificar um grupo de segurança de forma programática e no console do Guia do usuário do IAM.

Para criar uma política de permissão do IAM e anexá-la ao perfil de execução da função do Lambda

1. Em outra guia ou janela do navegador, abra a página Perfis do console do IAM.
2. Comece digitando o nome do perfil **`AutoEC2Termination`** e, quando ele aparecer na lista, escolha o nome do perfil.
3. Na página Resumo do perfil, escolha a guia Permissões e escolha o nome da política que já está anexada.
4. Na página Resumo da política, escolha Editar política.
5. Na guia Editor visual, escolha Adicionar mais permissões.
6. Em Serviço, escolha EC2.
7. Em Ações, escolha StopInstances. Você pode digitar **`Stop`** na barra de pesquisa e escolher `StopInstances` quando aparecer.
8. Em Recursos, escolha Todos os recursos, escolha Revisar política e, em seguida, selecione Salvar alterações.

   Isso cria automaticamente uma nova versão da política e define essa versão como padrão.

   Sua política final deve ser semelhante ao exemplo a seguir.

```
{
    "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:*"
        }
    ]
}
```

Etapa 3. Fazer um teste preliminar da sua função do Lambda

Nesta etapa, você envia um evento de teste para a sua função. A funcionalidade de teste do Lambda é feita enviando um evento de teste fornecido manualmente. A função processa o evento de teste como se o evento tivesse vindo EventBridge. Você pode definir vários eventos de teste com valores diferentes para exercitar todas as diferentes partes do seu código. Nesta etapa, você envia um evento de teste que indica que as tags de uma instância do Amazon EC2 foram alteradas e que as novas tags não incluem a chave e o valor da tag necessários.

Para testar a função do Lambda

1. Volte para a janela ou guia com o console Lambda e abra a guia Teste para sua função AutoEC2Termination.
2. Escolha Criar evento.
3. Em Nome do evento, insira **`SampleBadTagChangeEvent`**.
4. No Evento JSON, substitua o texto pelo evento de amostra apresentado no texto de exemplo a seguir. Você não precisa modificar as contas, a região ou o ID da instância para que esse evento de teste funcione corretamente.

```
{
  "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. Escolha Salvar e, em seguida, escolha Teste.

   O teste parece falhar, mas tudo bem.

   Você deve ver o seguinte erro na guia Resultados da execução, em Resposta.

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

   O erro ocorre porque a instância especificada no evento de teste não existe.

   As informações na guia Resultados da execução, na seção Registros de funções, demonstram que sua função do Lambda tentou parar com sucesso uma instância do EC2. No entanto, falhou

porque o código inicialmente tentou uma operação DryRun para interromper a instância, o que indicava que o ID da instância não era válido.

```
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. Para provar que o código não tenta interromper a instância quando a tag correta é usada, você pode criar e enviar outro evento de teste.

   Escolha a guia Teste acima da fonte do código. O console exibe seu evento SampleBadTagChangeEventde teste existente.

7. Escolha Criar evento.
8. Em Nome do evento, digite **`SampleGoodTagChangeEvent`**.
9. Na linha 17, exclua **`NOT-`** para alterar o valor para **`valid-value`**.

10. Na parte superior da janela Evento de teste, escolha Salvar e, em seguida, escolha Teste.

    A saída exibe o seguinte, o que demonstra que a função reconhece a tag válida e não tenta desligar a instância.

```
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
```

    Mantenha o console Lambda aberto em seu navegador.

Etapa 4. Crie a EventBridge regra que inicia a função

Agora você pode criar uma EventBridge regra que corresponda ao evento e aponte para sua função Lambda.

Para criar a EventBridge regra

1. Em outra guia ou janela do navegador, abra o EventBridge console na página Criar regra.
2. Em Nome, digite **`ec2-instance-rule`** e escolha Próximo.
3. Role para baixo até Método de criação e escolha Padrão personalizado (editor JSON).
4. Na caixa de edição, cole o texto padrão a seguir e escolha Próximo.

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

```
  }
}
```

Essa regra combina eventos `Tag Change on Resource` para instâncias do Amazon EC2 e invoca tudo o que você especificar como alvo na próxima etapa.

5. Em seguida, adicione a função do Lambda como destino. Na caixa Alvo 1, em Selecionar um destino, escolha função do Lambda.
6. Em Função, escolha a função AutoEC2Termination que você criou anteriormente e, em seguida, escolha Próximo.
7. Na página Configurar tags, escolha Próximo. Na página Revisar e criar, escolha Criar regra. Isso também concede automaticamente permissão para EventBridge invocar a função Lambda especificada.

Etapa 5. Testar a solução completa

Você pode testar seu resultado final criando uma instância do EC2 e observando o que acontece quando você altera suas tags.

Para testar a solução de monitoramento com uma instância real

1. Abra o console do Amazon EC2 na página Instâncias.
2. Crie uma instância do Amazon EC2. Antes de iniciá-la, anexe uma tag com a chave `valid-key` e o valor `valid-value`. Para obter informações sobre como criar e iniciar uma instância, consulte Etapa 1: Iniciar uma instância no Guia do usuário do Amazon EC2 para instâncias do Linux. No procedimento Para iniciar uma instância, na etapa 3, em que você insere a tag Nome, escolha também Adicionar tags adicionais, escolha Adicionar tag e, em seguida, insira a Chave de **`valid-key`** e o Valor de **`valid-value`**. Você pode continuar sem um par de chaves se essa instância for exclusivamente para os propósitos deste tutorial e você planeja excluí-la depois de finalizado. Retorne a este tutorial quando chegar ao final da Etapa 1; você não precisa fazer a Etapa 2: Conectar-se à sua instância.
3. Copie o InstanceIddo console.
4. Mude do console do Amazon EC2 para o console do Lambda. Escolha sua função AutoEC2Termination, escolha a guia Código e, em seguida, escolha a guia index.js para editar seu código.

5. Altere a segunda entrada na `InstanceList` colando o valor que você copiou do console do Amazon EC2. Verifique se o valor de `RegionToMonitor` corresponde à região que contém a instância que você colou.
6. Escolha Implantar para tornar suas alterações ativas. A função agora está pronta para ser ativada por meio de alterações de tag nessa instância na região especificada.
7. Mude do console do Lambda para o console do Amazon EC2.
8. Altere as tags anexadas à instância excluindo a tag de chave válida ou alterando o valor dessa chave.

> **Note**
>
> Para obter informações sobre como alterar as tags em uma instância do Amazon EC2 em execução, consulte Adicionar e excluir tags em um recurso individual no Guia do usuário do Amazon EC2 para instâncias do Linux.

9. Aguarde alguns segundos e, em seguida, atualize o console. A instância deve mudar seu estado de instância para Parando e depois para Parada.
10. Mude do console do Amazon EC2 para o console do Lambda com sua função e escolha a guia Monitor.
11. Escolha a guia Registros e, na tabela Invocações recentes, escolha a entrada mais recente na LogStreamcoluna.

    O CloudWatch console da Amazon abre a página Registrar eventos para a última invocação da sua função Lambda. A última entrada deve ser semelhante ao exemplo a seguir.

```
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
```

Resumo

Este tutorial demonstrou como criar uma EventBridge regra que corresponda a uma alteração de tag em um evento de recurso para instâncias do Amazon EC2. A regra apontava para uma função do Lambda que desliga automaticamente a instância se ela não tiver a tag necessária.

O EventBridge suporte da Amazon para alterações de tags em AWS recursos abre possibilidades para criar automação orientada por eventos em muitos. Serviços da AWS A combinação desse recurso com o AWS Lambda fornece a você ferramentas para criar soluções de tecnologia sem servidor que acessam os recursos da AWS com segurança, escalam sob demanda e são econômicas.

Outros casos de uso possíveis para o tag-change-on-resource EventBridge evento incluem:

- Lançar um aviso se alguém acessar seu recurso a partir de um endereço IP incomum: use uma tag para armazenar o endereço IP de origem de cada visitante que acessa o seu recurso. Alterações na tag geram um CloudWatch evento. Você pode usar esse evento para comparar o endereço IP de origem com uma lista de endereços IP válidos e ativar um e-mail de aviso se o endereço IP de origem não for válido.
- Monitore se há alterações no controle de acesso baseado em tags de um recurso — Se você configurou o acesso a um recurso usando o controle de acesso baseado em atributos (tag) (ABAC), você pode usar EventBridge eventos gerados por qualquer alteração na tag para solicitar uma auditoria por sua equipe de segurança.

Solução de problemas de alterações de tags

A lista de verificação a seguir poderá ser útil se ocorrerem erros ao tentar aplicar ou alterar tags em recursos selecionados nos resultados da consulta Encontrar recursos para marcar.

- O recurso talvez já tenha o número máximo de tags. Geralmente, os recursos podem ter um máximo de 50 tags definidas pelo usuário. As tags geradas pela AWS não contam para o máximo de 50 tags. Outros usuários também podem estar adicionando tags ao mesmo recurso ao mesmo tempo, o que pode aumentar as tags do recurso para o número máximo.

- Alguns serviços permitem um conjunto de caracteres diferente (ou restringem o conjunto de caracteres que é permitido) para a criação de tags. Se você tiver adicionado ou alterado tags usando caracteres especiais, analise os requisitos de tags na documentação do serviço do recurso para verificar se esses caracteres são permitidos pelo serviço.
- Talvez você não tenha permissões para modificar as tags do recurso. Se você não tiver permissões para visualizar as tags existentes em um recurso, não poderá fazer alterações nas tags do recurso.
- Talvez você não tenha as permissões para alterar o recurso. As alterações nos metadados do recurso podem estar restringidas por outro administrador.
- O recurso pode ter sido editado ou excluído por outro usuário ou processo. Por exemplo, suponha que um recurso tenha sido lançado como parte da criação de uma pilha AWS CloudFormation. Se a pilha foi excluída ou não está mais em um estado ativo, o recurso pode não estar mais disponível.
- As alterações de tags poderão não ser possíveis se um recurso estiver offline ou encerrado, ou se outras atualizações (por exemplo, atualizações de software) no recurso estiverem em andamento.
- As alterações de tags podem falhar se você fechar a guia do navegador ou alterar a página antes que as alterações de tags estejam concluídas. Permita que as alterações de tags sejam concluídas e aguarde até que o banner de sucesso ou de falha apareça na página, antes de sair da página.
- Embora haja um limite de taxa para o AWS Resource Groups Tagging API, o serviço que você está marcando pode impor um limite separado que você pode atingir antes do limite da API de marcação de grupos de recursos.

Informações relacionadas

- Usar tags de alocação de custos no Guia do usuário do AWS Billing

Segurança no Tag Editor

A segurança de nuvem na AWS é prioridade máxima. Como cliente da AWS, você contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa os Serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programsAWS. Para saber mais sobre os programas de conformidade aplicáveis ao Tag Editor, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem - sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Tag Editor. Os tópicos a seguir mostram como configurar o Tag Editor para atender aos seus objetivos de segurança e conformidade.

Tópicos

Proteção de dados no Tag Editor

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no Tag Editor. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo

hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja asConta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui trabalhar com o Tag Editor ou outros Serviços da AWS usando o console, a API, a AWS CLI ou os SDKs da AWS. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados

As informações de atribuição de tags não são criptografadas. Embora não sejam criptografadas, as tags podem conter informações usadas como parte de sua estratégia de segurança, por isso é

importante controlar quem pode acessar as tags nos recursos. É especialmente importante que você controle quem pode modificar as tags, pois esse acesso pode ser usado para elevar as permissões de alguém.

Criptografia inativa

Não há outras formas de isolar o tráfego do serviço ou da rede que sejam específicas ao Tag Editor. Se aplicável, use isolamento específico da AWS. É possível usar o console e a API do Tag Editor em uma nuvem privada virtual (VPC) para ajudar a maximizar a privacidade e a segurança da infraestrutura.

Criptografia em trânsito

Os dados do Tag Editor são criptografados em trânsito para o banco de dados interno do serviço para backup. Isso não é configurável pelo usuário.

Gerenciamento de chaves

Atualmente, o Tag Editor não está integrado com o AWS Key Management Service e não oferece suporte AWS KMS keys.

Privacidade do tráfego entre redes

O Tag Editor usa HTTPS para todas as transmissões entre usuários do Tag Editor e a AWS. O Tag Editor usa o Transport Layer Security (TLS) 1.3, mas também é compatível com o TLS 1.2.

Gerenciamento de identidade e acesso para o Tag Editor

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar recursos do Tag Editor. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Solução de problemas de identidade e acesso do Tag Editor

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho realizado no Tag Editor.

Usuário do serviço: se você usa o serviço Tag Editor para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do Tag Editor para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Tag Editor, consulte Solução de problemas de identidade e acesso do Tag Editor.

Administrador do serviço: se você for o responsável pelos recursos do Tag Editor na sua empresa, provavelmente terá acesso total ao Tag Editor. Cabe a você determinar quais funcionalidades e recursos do Tag Editor os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a sua empresa pode usar o IAM com o Tag Editor, consulte Como o Tag Editor funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Tag Editor. Para visualizar exemplos de políticas baseadas em identidade do Tag Editor que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade do Tag Editor.

Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários do IAM Identity Center, a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades utilizando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no AWS Management Console ou no de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na AWS, consulte Conta da AWS Como fazer login na sua no Início de Sessão da AWS Guia do usuário.

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Usuários e grupos

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível utilizar grupos para especificar permissões para vários

usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, é possível ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Funções

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar uma função para um provedor de identidade de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.

- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou uma função vinculada ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Perfil vinculado a serviço: um perfil vinculado a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar uma função do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API da AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS aceita tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada .Usuário raiz da conta da AWS Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) noAWS Organizations Guia do usuário do .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliaçãode políticas no Guia do usuário do IAM.

Como o Tag Editor funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Tag Editor, você precisa saber quais atributos do IAM estão disponíveis para uso com o Tag Editor. Para ter uma visão de alto nível de como o Tag Editor e outros Serviços da AWS funcionam com o IAM, consulte Serviços da AWS esse trabalho com o IAM no Guia do usuário do IAM.

Tópicos

- Políticas baseadas em identidade do Tag Editor
- Políticas baseadas em recursos
- Autorização baseada em tags do
- Perfis do IAM do Tag Editor

Políticas baseadas em identidade do Tag Editor

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, além das condições sob as quais as ações são permitidas ou negadas. O Tag Editor oferece suporte a ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política no Tag Editor usam o seguinte prefixo antes da ação: `tag:`. As ações do Tag Editor são executadas inteiramente no console, mas têm o prefixo `tag` nas entradas do log.

Por exemplo, para conceder a alguém permissão para marcar um recurso com a operação da API `tag:TagResources`, inclua a ação `tag:TagResources` na política da pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Tag Editor define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações de marcação em uma única declaração, separe-as com vírgulas, conforme a seguir.

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

Você também pode especificar várias ações utilizando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Get`, inclua a ação a seguir:

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

Para visualizar uma lista de ações do Tag Editor, consulte Ações, recursos e chaves de condição para o Tag Editor na Referência de autorização do serviço.

Recursos

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

O Tag Editor não tem recursos próprios. Em vez disso, ele manipula os metadados (tags) anexados aos recursos criados por outros Serviços da AWS.

Chaves de condição

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condiçãoAWS global no Guia do usuário do IAM.

O Tag Editor não oferece chaves de condição específicas ao serviço.

Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Tag Editor, consulte Exemplos de políticas baseadas em identidade do Tag Editor.

Políticas baseadas em recursos

O Tag Editor não é compatível com políticas baseadas em recursos porque não define recursos próprios.

Autorização baseada em tags do

A autorização baseada em tags faz parte da estratégia de segurança chamada controle de acesso por atributo (ABAC).

Para controlar o acesso a um recurso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Você pode aplicar tags a um recurso ao criar ou atualizar o recurso.

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um atributo baseado em tags desse atributo, consulte Visualizar grupos com base em tags. Para obter mais informações sobre controle de acesso baseado em atributos (ABAC), consulte Para que serve o ABAC? AWSno Guia do usuário do IAM.

Perfis do IAM do Tag Editor

Uma função do IAM é uma entidade dentro da sua Conta da AWS que tem permissões específicas. O Tag Editor não tem nem usa perfis de serviço.

Usar credenciais temporárias com o Tag Editor

No Tag Editor, é possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

Perfis vinculados ao serviço

As funções vinculadas ao serviço permitem Serviços da AWS acessar recursos em outros serviços para concluir uma ação em seu nome.

O Tag Editor não tem nem usa perfis vinculados ao serviço.

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome.

O Tag Editor não tem nem usa perfis de serviço.

Exemplos de políticas baseadas em identidade do Tag Editor

Por padrão, as entidades principais, como perfis e usuários, não têm permissão para criar ou modificar tags. Elas também não podem executar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou APIs da AWS. Um administrador do IAM deve criar políticas do IAM que concedam às entidades principais permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas às entidades principais que exigem essas permissões.

Para obter instruções sobre como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Práticas recomendadas de políticas
- Usar o console do Tag Editor e a API de marcação de grupos de recursos
- Permitir que os usuários exibam as próprias permissões
- Visualizar grupos com base em tags

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Tag Editor em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. É possível também usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condição no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar o console do Tag Editor e a API de marcação de grupos de recursos

Para acessar o console do Tag Editor e a API de marcação de grupos de recursos, você deve ter um conjunto mínimo de permissões. Essas permissões devem autorizar você a listar e visualizar detalhes sobre as tags anexadas aos recursos na sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console e os comandos de API não funcionarão como pretendido para as entidades principais do IAM com essa política.

Para garantir que essas entidades principais ainda possam usar o Tag Editor, anexe a política a seguir (ou uma política que contenha as permissões listadas na política a seguir) às entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

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

Para obter mais informações sobre como conceder acesso ao Tag Editor e à API de marcação de grupos de recursos, consulte Conceder permissões para usar o Tag Editor.

Permitir que os usuários exibam as próprias permissões

Este exemplo mostra como é possível criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política

inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a AWS API.

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

Visualizar grupos com base em tags

Você pode usar condições em sua política baseada em identidade para controlar o acesso aos recursos do Tag Editor com base em tags. Este exemplo mostra como você pode criar uma política que permite visualizar um recurso, neste exemplo, um grupo de recursos. No entanto, a permissão é

concedida somente se a tag do grupo `project` tiver o mesmo valor que a tag `project` anexada à entidade principal da chamada.

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

Você pode anexar essa política aos usuários na sua conta. Se um usuário com a chave de tag `project` e o valor de tag `alpha` tentar visualizar um grupo de recursos, o grupo também deverá ser marcado como `project=alpha`. Caso contrário, o usuário terá o acesso negado. A chave da tag de condição `project` corresponde a `Project` e a `project` porque os nomes das chaves de condição não fazem distinção entre maiúsculas e minúsculas. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

Solução de problemas de identidade e acesso do Tag Editor

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Tag Editor e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Tag Editor
- Não estou autorizado a realizar iam: PassRole

Não tenho autorização para executar uma ação no Tag Editor

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. Seu administrador é a pessoa que forneceu a você suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário `mateojackson` tenta usar o console para visualizar tags em um recurso, mas não tem as permissões `tag:GetTagKeys`.

```
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
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `my-test-resource` usando a ação `tag:GetTagKeys`.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Tag Editor.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um novo perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Tag Editor. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Registrar em log e monitorar no Tag Editor

Todas as ações do Tag Editor estão registradas em log no AWS CloudTrail.

Registrando chamadas da API do Tag Editor com CloudTrail

O Tag Editor é integrado comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS) no Tag Editor. CloudTrail captura todas as chamadas de API para o Tag Editor como eventos, incluindo chamadas do console do Tag Editor e de chamadas de código para a API Resource Groups Tagging. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Tag Editor. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Tag Editor, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações do Editor de tags em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Editor de tags ou no console do Tag Editor, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para obter um registro contínuo de eventos em sua Conta da AWS, inclusive eventos para o Tag Editor, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte os seguintes recursos do :

- Criar uma trilha para a sua Conta da AWS
- Serviços e integrações compatíveis com o CloudTrail
- Configurando notificações do Amazon SNS para CloudTrail

- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Tag Editor são registradas CloudTrail e documentadas na Referência da API Tag Editor. As ações do Editor de Tags no console são registradas CloudTrail e mostradas como eventos com `tagging.amazonaws.com` o. `eventSource`

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte o CloudTrail`userIdentity`elemento.

Noções básicas sobre entradas de arquivos de log para o Tag Editor

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a ação`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"
    }
```

```
}
```

Validação de conformidade do Tag Editor

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade em que você está interessado. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes atributos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services: esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).

- Avaliar recursos com regras no AWS ConfigGuia do desenvolvedor do : o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub - Este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager – Esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no Tag Editor

O Tag Editor realiza backups automáticos nos recursos internos do serviço. Esses backups não são configuráveis pelo usuário. Os backups são criptografados, tanto em repouso quanto em trânsito. O Tag Editor armazena dados de clientes no Amazon DynamoDB.

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as Zonas de Disponibilidade, você pode projetar e operar aplicativos e bancos de dados que executam o failover automaticamente entre as Zonas de Disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Se você excluir tags acidentalmente, entre em contato com a Central do AWS Support.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura global da AWS.

Segurança da infraestrutura no Tag Editor

O Tag Editor não fornece formas adicionais de isolar o tráfego de serviços ou de rede. Se aplicável, use isolamento específico da AWS. É possível usar o console e a API do Tag Editor em uma nuvem privada virtual (VPC) para ajudar a maximizar a privacidade e a segurança da infraestrutura.

Você usa chamadas de API publicadas pela AWS para acessar o Tag Editor por meio da rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TSL 1.2 e recomendamos TSL 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do AWS Identity and Access Management (IAM). Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

O Tag Editor não oferece suporte a políticas baseadas em recursos.

É possível chamar essas operações de API do Tag Editor de qualquer local da rede, mas o Tag Editor não é compatível com políticas de acesso baseadas em recursos, que podem incluir restrições com base no endereço IP de origem. Também é possível usar políticas do Tag Editor para controlar o acesso de endpoints da Amazon Virtual Private Cloud (Amazon VPC) ou de VPCs específicas. Efetivamente, essa abordagem isola o acesso à rede para um determinado recurso a partir somente da VPC específica dentro da rede da AWS.

Informações de referência do Tag Editor

As informações de referência do Tag Editor incluem as Service Quotas aplicáveis.

Service Quotas para o Tag Editor

A tabela a seguir fornece informações sobre as Service Quotas do Tag Editor.

No momento, essas cotas não são ajustáveis usando o console de Service Quotas. Entre em contato com a AWS Support.

Nome	Padrão
Tags anexadas por recurso	50 tags definidas pelo usuário (as tagsAWS geradas não contam nesse limite).
Nome da chave da tag	Mínimo de 1, máximo de 128 caracteres Unicode em UTF-8. Os caracteres permitidos incluem letras, números, espaços e os seguintes caracteres: `_ . : / = + - @` Os nomes das chaves não podem começar `aws:` porque esse prefixo está reservado para AWS uso. **Note** Alguns Serviços da AWS têm algumas restrições adicionais de caracteres

Nome	Padrão
	ou comprimento. Para obter detalhes, consulte a documentação do serviço específico.
Valores de tag	Mínimo de 0, máximo de 256 caracteres Unicode em UTF-8. Os caracteres permitidos incluem letras, números, espaços e os seguintes caracteres: `_ . : / = + - @` **Note** Alguns Serviços da AWS têm algumas restrições adicionais de caracteres ou comprimento. Para obter detalhes, consulte a documentação do serviço específico.
Taxa de chamada da operação de API GetResources	Número máximo de 15 chamadas por segundo

Nome	Padrão	
Taxa de chamada das seguintes operações de API: • TagResources • UntagResources • GetTagKeys • GetTagValues	Número máximo de 5 chamadas por segundo	

Histórico de documentos do Tag Editor

Alteração	Descrição	Data
Conteúdo de marcação transferido de Referência geral da AWS para este guia	Os tópicos sobre a marcação de seus recursos da AWS foram transferidos do Referência geral da AWS para este guia.	24 de março de 2023
Atualização de práticas recomendadas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	3 de janeiro de 2023
Documentação do Tag Editor movida para seu próprio guia	A documentação do Tag Editor agora é fornecida em seu próprio guia do usuário, em vez de fazer parte do Guia do usuário do AWS Resource Groups.	13 de dezembro de 2022
Verificar a conformidade com as políticas de tag	Depois de criar e anexar políticas de tags às contas que usam o AWS Organizations, você pode encontrar tags não compatíveis em recursos nas contas da sua organização.	26 de novembro de 2019
O Tag Editor agora é compatível com a descoberta de recursos não marcados	Agora você pode pesquisar recursos no Tag Editor que não têm valores de tag para uma determinada chave de tag.	18 de junho de 2019

O console do é transferido para fora do console do AWS Systems Manager	O console do Tag Editor agora é independente do console do Systems Manager. Embora você ainda possa encontrar ponteiros para o console do Tag Editor na barra de navegação esquerda do Systems Manager, você pode abrir o console do Tag Editor diretamente no menu suspenso no canto superior esquerdo do AWS Management Console.	5 de junho de 2019
Ferramentas do Tag Editor herdadas e mais antigas não estão mais disponíveis	Menções sobre Tag Editor mais antigo, clássico ou herdado foram removidas; essas ferramentas não estão mais disponíveis na AWS. Em vez disso, use o Tag Editor.	14 de maio de 2019
O Tag Editor agora é compatível com recursos de marcação em várias regiões	O Tag Editor agora permite pesquisar e gerenciar tags de recursos em várias regiões, com sua região atual adicionada às consultas de recursos por padrão.	2 de maio de 2019

O Tag Editor agora oferece suporte à exportação dos resultados da consulta para um CSV	Você pode exportar os resultados de uma consulta na página Localizar recursos a serem marcados para um arquivo em formato CSV. Uma nova coluna Região é mostrada nos resultados de consultas do Tag Editor. O Tag Editor agora permite pesquisar recursos que têm valores vazios para uma determinada chave de tag. Os valores de chaves de tags são preenchidos automaticamente conforme você digita um valor exclusivo entre chaves existentes.	2 de abril de 2019
O Tag Editor agora é compatível com a adição de todos os tipos de recurso a uma consulta	Você pode aplicar tags a até 20 tipos de recurso individua is em uma única operação, ou escolher Todos os tipos de recurso para consultar todos os tipos de recurso em uma região. O preenchimento automático foi adicionado ao campo Chave de tag de uma consulta para ajudar a habilitar chaves de tags consisten tes entre recursos. Se as alterações de tags falharem em alguns recursos, você poderá tentar novamente as alterações de tags apenas nos recursos nos quais as alterações de tags falharam.	19 de março de 2019

O Tag Editor agora oferece suporte a vários tipos de recurso em uma pesquisa	Você pode aplicar tags a até 20 tipos de recurso em uma única operação. Você também pode escolher as colunas que são mostradas nos resultados de pesquisa, incluindo colunas para cada chave de tag exclusiva encontradas nos resultados da pesquisa ou recursos selecionados dos resultados.	26 de fevereiro de 2019

AWS Glossário

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.