Manual do usuário

AWS Recursos de marcação e editor de tags

Versão 1.0

AWS Recursos de marcação e editor de tags: Manual do usuário

Table of Contents

O que é o Tag Editor?

O Tag Editor permite que você gerencie tags de forma eficaz. As tags são pares de chaves e valores que atuam como metadados para organizar seus AWS recursos. Com a maioria dos AWS recursos, 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 uma entrada secreta. 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 os recursos por finalidade, proprietário, ambiente ou outros critérios.

Cada tag da tem duas partes:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). As chaves de tag diferenciam maiúsculas de minúsculas
- Um valor de tag (por exemplo, `111122223333` ou `Production`). Assim como as chaves de tag, os valores de tag diferenciam maiúsculas de minúsculas.

> **Note**
>
> Embora as chaves de tag diferenciem maiúsculas e minúsculas, o IAM utiliza validações adicionais para seus próprios recursos a fim de evitar a aplicação de chaves de tag que diferem apenas em maiúsculas e minúsculas. Recomendamos não usar chaves que diferem apenas em maiúsculas e minúsculas. Consulte Tags para recursos do IAM para obter mais informações.

Métodos de marcação de recursos

Há três maneiras de adicionar tags aos seus AWS recursos:

- AWS service (Serviço da AWS) Operação de API — As operações de API de marcação suportaram diretamente um AWS service (Serviço da AWS). Para descobrir qual funcionalidade de marcação cada uma AWS service (Serviço da AWS) fornece, consulte a documentação do serviço no índice da AWS documentação.
- Console do Tag Editor: alguns serviços também permitem a marcação por meio do console do Tag Editor.
- 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.

> **Note**
>
> Você também pode usar a AWS Service Catalog TagOptions Biblioteca para gerenciar facilmente as tags em produtos provisionados. A TagOptioné um par de valores-chave gerenciado no Service Catalog. Não é uma AWS tag, mas serve como um modelo para criar uma AWS tag com base na TagOption.

É possível etiquetar recursos para todos os serviços que aumentam os custos na AWS. Para os serviços a seguir, AWS recomenda uma alternativa mais recente Serviços da AWS que ofereça suporte à marcação para melhor atender aos casos de uso do cliente.

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

Saiba mais

Esta página fornece informações gerais sobre AWS recursos de marcação. Para obter mais informações sobre a marcação de recursos em um AWS serviço específico, consulte sua 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 Resource Groups Tagging.
- Para obter informações sobre a funcionalidade de marcação que cada um AWS service (Serviço da AWS) fornece, consulte a documentação do serviço no índice da AWS documentação.
- Para obter informações sobre o uso de tags nas políticas do IAM para ajudar a controlar quem pode visualizar e interagir com seus AWS recursos, consulte Controle do acesso a e para usuários e funções do IAM usando tags no Guia do usuário do IAM.

Estratégias e práticas recomendadas

Essas seções fornecem informações sobre estratégias e práticas recomendadas para marcar recursos da AWS e usar o Tag Editor.

práticas recomendadas de marcação

Ao criar uma estratégia de marcação para AWS recursos, siga as melhores práticas:

- Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags podem ser acessadas por vários AWS serviços, 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 .

práticas recomendadas de nomenclatura de tags

Essas são várias práticas recomendadas e convenções de nomenclatura que recomendamos que você use com suas tags. Consulte Tags de nomenclatura no Guia do usuário do IAM para obter mais informações.

Várias tags são predefinidas AWS ou criadas automaticamente por várias 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 EC2 spot da Amazon que iniciou a instância.
- `aws:cloudformation:stack-name` é uma tag que identifica a pilha do 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 conforme definido por sua organização e não por AWS 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`.

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 possuir apenas um valor.
- A chave da 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 AWS serviço. Para obter informações sobre quais caracteres você pode usar para marcar recursos em um AWS serviço específico, consulte sua 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 alocação de custos
- Tags para automação
- Tags para controle de acesso
- Governança de marcação

Tags para organização de recursos

As tags são uma boa maneira de organizar AWS recursos no Console de gerenciamento da AWS. É possível configurar tags para serem exibidas com recursos, além de pesquisar e filtrar por tags. Com o AWS Resource Groups serviço, você pode criar grupos de AWS recursos com base em uma ou mais tags ou partes de tags. Você também pode criar grupos com base em sua ocorrência em uma AWS CloudFormation pilha. 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

AWS O Cost Explorer e os relatórios detalhados de faturamento permitem que você divida AWS os custos por tag. Normalmente, você usa etiquetas comerciais, como center/business unidade de custo, cliente ou projeto, para associar AWS custos às 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.

Para alguns serviços, você pode usar uma `createdBy` tag AWS gerada para fins de alocação de custos, para ajudar a contabilizar recursos que, de outra forma, poderiam não ser 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 Gerenciamento de Faturamento e Custos da AWS .

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 tags de

instância do Amazon Elastic Compute Cloud (Amazon EC2) são uma forma simples de identificar instâncias para optar por não participar dessa 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 função do IAM podem incluir condições para limitar as chamadas de EC2 API a ambientes específicos (como desenvolvimento, teste ou produção) com base em suas tags. 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 eficaz usa tags padronizadas e as aplica de forma consistente e programática em todos os recursos. AWS Você pode usar abordagens reativas e proativas para controlar as tags em seu AWS ambiente.

- A governança reativa serve para encontrar recursos que não estão devidamente marcados usando ferramentas como a API Resource Groups Tagging e Regras do AWS Config 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 Service Catalog CloudFormation, políticas de tags ou permissões em AWS Organizations nível de recurso do IAM para garantir que as tags padronizadas sejam aplicadas de forma consistente na criação do recurso.

  Por exemplo, você pode usar a CloudFormation `Resource Tags` propriedade 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.

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

Conceitos básicos sobre o Tag Editor

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

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 Console de gerenciamento da AWS.
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, AWS informe-o escolhendo 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

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

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. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo 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 recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso 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 Console de gerenciamento da AWScomo 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 do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   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 com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

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

   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 Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

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

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

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 do AWS 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 Tag Editor

Para usar o console do Tag Editor para listar e marcar recursos, as permissões a seguir devem ser adicionadas a uma declaração de política de usuário no IAM. Você pode adicionar políticas AWS gerenciadas que são mantidas e AWS atualizadas 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 observação Importante a seguir.

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 observação Importante a seguir.

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.

  JSON

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

  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).

JSON

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

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 permissão `resource-groups:SearchResources` possibilita que o Tag Editor liste recursos quando você filtra sua pesquisa usando chaves ou valores de tag.

A permissão `resource-explorer:ListResources` possibilita que o Tag Editor 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 Adicionar permissões.
4. Escolha Anexar políticas existentes diretamente.
5. Escolha Criar política.
6. Na guia JSON, cole a seguinte declaração de política.

   JSON

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

> **Note**
>
> 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 em nível de recurso nas políticas — Muitos serviços oferecem suporte ao uso ARNspara 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? AWS no Guia do AWS 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 do AWS 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

Encontrar recursos para marcar

Com o Tag Editor, você cria uma consulta para encontrar recursos em uma ou mais Regiões da AWS que estão 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 o Regiões da AWS em que 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. 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).

> **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 em 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 com tag. 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.

Visualizar e editar tags existentes de um recurso selecionado

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

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 obter 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 “–”.

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 com tags, 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 com tags para um arquivo de valores separados por vírgulas (.csv). O arquivo.csv inclui os nomes dos recursos, serviços, região, recurso IDs, 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 navegador, escolha abrir o arquivo .csv ou salvá-lo em um local conveniente.

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 marcação usando o Editor de tags no. Console de gerenciamento da AWS No entanto, você também pode gerenciar as tags em seus AWS recursos usando as seguintes ferramentas:

- Você pode digitar ou programar comandos no prompt do shell usando os comandos da `resourcegroupstaggingapi` na 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 disponíveis AWS SDKsusando a marcação de grupos de recursos APIs, como a marcação para APIs Python ou a marcação para Java. APIs

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 com tags. Você pode selecionar até 500 recursos nos quais gerenciar tags.

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 obter mais informações, consulte Visualizar e editar tags existentes de 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 com tags, 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.
3. Marque a caixa de seleção de um ou mais recursos e depois escolha Gerenciar tags dos recursos selecionados.
4. Na página Manage tags (Gerenciar tags), 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. AWS as tags geradas 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 obter 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.
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 obter 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.

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 obter mais informações, consulte the section called “Tentar novamente as alterações de tags com falha”.

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 AWS recursos. Toda tentativa de acessar um AWS serviço ou ler ou gravar um AWS recurso 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.

Tags e controle de acesso baseado em atributo

As tags podem ser uma parte importante da sua estratégia de controle de AWS acesso. Para obter informações sobre o uso de tags como atributos em uma estratégia de controle de acesso baseado em atributos (ABAC), consulte Controle do acesso a AWS recursos usando tags e Controle do acesso a e para usuários e funções 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: Defina permissões para acessar AWS recursos com base em tags no Guia do AWS Identity and Access Management usuário.

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 .

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	Description
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.

JSON

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

Example 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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
```

```
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
      }
    }
  ]
}
```

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 :

- Controle do acesso aos AWS recursos usando tags
- Controlar acesso para usuários e perfis do IAM usando tags
- Tutorial do IAM: defina permissões para acessar AWS recursos com base em tags — Mostra como conceder acesso a diferentes projetos e grupos usando várias tags.

AWS Organizations políticas de tags

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.

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.

Tópicos

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 recurso e criar e anexar políticas de tag. AWS Organizations 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 do Leste dos Região da AWS 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 AWS Identity and Access Management (IAM) a seguir fornece permissões para avaliar a conformidade de tags de uma conta.

JSON

```
{
    "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.
- `s3:ListAllMyBuckets`: para ajudar a acessar o relatório de conformidade em toda a organização.
- `s3:GetBucketAcl`: para inspecionar a lista de controle de acesso (ACL) do bucket do Amazon S3 que recebe o relatório de conformidade.
- `s3:GetObject`: para recuperar o relatório de conformidade do bucket do Amazon S3 de propriedade do serviço.
- `s3:PutObject`: para colocar o relatório de conformidade no bucket do Amazon S3 especificado.

Se o bucket do Amazon S3 em que o relatório está sendo entregue for criptografado via SSE-KMS, você também deverá ter a `kms:GenerateDataKey` permissão para esse bucket.

O exemplo de política do IAM a seguir fornece permissões para avaliar a conformidade em toda a organização. Substitua cada um *`placeholder`* por suas próprias informações:

- *`bucket_name`*: nome do bucket do Amazon S3.
- *`organization_id`*: ID da sua organização.

JSON

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

```
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/
*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
            }
        }
    ]
}
```

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, a identidade que você usa para chamar a API `StartReportCreation` deve ter acesso a um bucket do Amazon Simple Storage Service (Amazon S3) na região Leste dos EUA (Norte da Virgínia) para armazenar o relatório. As políticas de tag usam as credenciais da identidade de chamada para entregar o relatório de conformidade ao bucket especificado.

Se o bucket e a identidade que estão sendo usados para chamar a API `StartReportCreation` pertencerem à mesma conta, políticas adicionais de bucket do Amazon S3 não serão necessárias para esse caso de uso.

Se a conta associada à identidade usada para chamar a API `StartReportCreation` for diferente da conta proprietária do bucket do Amazon S3, a política de bucket a seguir deverá ser anexada ao bucket. Substitua cada um *`placeholder`* por suas próprias informações:

- *`bucket_name`*: nome do bucket do Amazon S3.
- *`organization_id`*: ID da sua organização.
- *`identity_ARN`*: o ARN da identidade do IAM usada para chamar a API `StartReportCreation`.

JSON

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

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 não marcados em sua conta, use Explorador de recursos da AWS com uma consulta que usa**`tag:none`**. Para obter mais informações, consulte Pesquisar 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 tags a uma unidade organizacional (OU), ela se aplica a todas as contas OUs que pertencem à OU.

> **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 quais 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 exibidos 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) em que 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, AWS API)

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 tags no AWS CLI, consulte Usando políticas de tag AWS CLI no Guia do AWS Organizations usuário.
- 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 obter 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 não marcados em sua conta, use Explorador de recursos da AWS com uma consulta que usa**`tag:none`**. Para obter mais informações, consulte Pesquisar 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 sua organização `us-east-1` Região da AWS somente no. 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:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

Para ver um exemplo de política do IAM exibindo essas permissões, examine Permissions for evaluating organization-wide compliance.

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.

> **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 um Conta da AWS que era membro da organização, ele poderá continuar aparecendo no relatório de conformidade da tag por até 90 dias.

Para gerar um relatório de conformidade em toda a organização (API)AWS CLI 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 tags no AWS CLI, consulte Usando políticas de tag AWS CLI no Guia do AWS Organizations usuário.
- AWS API:
  - 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 AWS Lambda função para invocar fluxos de trabalho automatizados. Este tópico fornece um tutorial sobre como usar o Lambda para criar uma solução econômica sem servidor para processar com segurança as alterações de tags em seus recursos. 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 AWS recursos oferecem suporte a tags, que são atributos personalizados definidos pelo usuário para organizar e categorizar AWS recursos 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 continuamente pesquisado APIs e orquestrado várias chamadas. Agora, qualquer alteração em uma tag, incluindo o serviço individual APIs, o Editor de tags e a API de marcação, iniciará a alteração da 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 Amazon Resource Names (ARNs) que identificam os recursos 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

AWS Lambda segue o paradigma 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. Sem servidor, nesse contexto, significa que você não precisa provisionar, configurar ou gerenciar os servidores usados para executar seu código. 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

À medida que seu pool de AWS recursos e o Contas da AWS que você gerencia cresce, 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 AWS recursos 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 instâncias IDs. Você deve atualizar a lista com a instância IDs que deseja encerrar para o teste. Isso ajuda a garantir que você não possa desligar acidentalmente todas as instâncias em uma região do seu 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 à instância IDs na lista.

Este exemplo usa JavaScript e a versão 16.x do Node.js. O exemplo usa o Conta da AWS ID de exemplo 123456789012 e o Leste dos Região da AWS 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.

Tópicos

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 do zero.
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 estiver aberta, clique com o botão direito do mouse no arquivo index.js na pasta Auto EC2 Terminator 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. A função AWS fornecida lambda_basic_executionnão 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.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/
lambda/AutoEC2Termination:*"
        }
    ]
}
```

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 de EC2terminação automática.
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 Logs da função, 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 Origem 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 do 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 de EC2encerramento automático que você criou anteriormente e, em seguida, escolha Avançar.
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 ter informações sobre como criar e iniciar uma instância, consulte Etapa 1: executar uma instância no Manual do usuário do Amazon EC2. 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 de EC2terminação automática, 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 ter informações sobre como alterar as tags em uma instância do Amazon EC2 em execução, consulte Add and delete tags on an individual resource no Manual do usuário do Amazon EC2.

9. Aguarde alguns segundos e, em seguida, atualize o console. A instância deve mudar seu estado de instância para Interrompendo e depois para Interrompida.
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 do Tutorial

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 AWS Lambda fornece ferramentas para criar soluções sem servidor que acessam AWS recursos 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 no máximo 50 tags definidas pelo usuário. AWS as tags geradas 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 do 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 Resource Groups Tagging.

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.

Segurança no Tag Editor

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. 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 programas de conformidade da AWS. 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 AWS compartilhada se aplica à proteção de dados no Editor de tags. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global

que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o 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 Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou 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) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão 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 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Tag Editor ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em 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, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse 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 em repouso

Não há outras formas de isolar o tráfego do serviço ou da rede que sejam específicas ao Tag Editor. Se aplicável, use isolamento AWS específico. 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

No momento, o Tag Editor não está integrado 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. 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

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. 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 você pode usar sem custo adicional.

Tópicos

- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o Tag Editor funciona com o IAM
- Exemplos de políticas baseadas em identidade do Tag Editor
- Solução de problemas de identidade e acesso do Tag Editor

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso do Tag Editor).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como o Tag Editor funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade do Tag Editor)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como AWS IAM Identity Center (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente

recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Usuários e grupos

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e 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. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, 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 AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de 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 recursos 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 podem ser usadas para permitir ou negar acesso em uma política. 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um 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` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS 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 recurso baseado em tags desse recurso, 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? AWS no 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. Eles também não podem realizar tarefas usando o Console de gerenciamento da AWS, AWS Command Line Interface (AWS CLI) ou AWS APIs. 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 política

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 sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções 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 saber mais 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. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation.

Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia 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 cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais 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 permitir que você liste e visualize detalhes sobre as tags anexadas aos recursos em seu 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 Adição de permissões a um usuário no Guia do usuário do IAM.

JSON

```
{
  "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 visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita 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 programaticamente usando a API AWS CLI ou AWS .

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

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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.

JSON

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

```
    ]
}
```

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 isso Console de gerenciamento da AWS indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu 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 uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada 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 precisar de ajuda, entre em contato com seu AWS administrador. 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 logadas AWS CloudTrail.

Registrando chamadas da API do Tag Editor com CloudTrail

O Tag Editor é integrado com AWS 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 visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo 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 AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para saber mais, consulte os seguintes recursos:

- Criando uma trilha para o seu 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 CloudTrail registradas por 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 usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil 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 origem e inclui informações sobre a ação solicitada, a data e hora da ação, parâmetros de solicitação, e assim por diante. arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas da API pública. Assim, elas não são exibidas 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 dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a documentação AWS de segurança.

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 AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações 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 data center tradicionais.

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

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

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 AWS específico. 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 AWS publicadas para acessar o Tag Editor pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TSL 1.2 e recomendamos TSL 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve 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 de chave de acesso e uma chave de acesso secreta associada a um principal 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. Você também pode usar as políticas do Tag Editor para controlar o acesso de endpoints específicos ou específicos da Amazon Virtual Private Cloud (Amazon VPC). VPCs Efetivamente, essa abordagem isola o acesso à rede a um determinado recurso somente da VPC específica dentro da AWS rede.

Cotas de serviço

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 Suporte.

Name	Padrão
Tags anexadas por recurso	50 tags definidas pelo usuário (as tags AWS 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 com `aws:` porque esse prefixo está reservado para AWS uso. **Note** Alguns Serviços da AWS têm algumas restrições adicionais de caracteres ou comprimento. Para obter detalhes, consulte a documenta

Name	Padrão
	ção 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 ligação para o GetResources Operação de API	Número máximo de 15 chamadas por segundo

Name	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
Permissões atualizadas para avaliar a conformidade em toda a organização	Atualização das permissões para avaliar a conformidade em toda a organização e incluir permissões que auxiliam no acesso ao relatório de conformidade.	28 de agosto de 2024
Conteúdo atualizado	Títulos de tópicos atualizados e conteúdo reorganizado para melhorar a legibilidade e facilitar a descoberta.	25 de julho de 2024
Marcar conteúdo de Referência geral da AWS movido para este guia	Os tópicos sobre a marcação de seus AWS recursos 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 AWS Resource Groups do usuário.	13 de dezembro de 2022
Verificar a conformidade com as políticas de tag	Depois de criar e anexar políticas de tags às contas	26 de novembro de 2019

	que usam AWS Organizations, você pode encontrar tags não compatíveis em recursos nas contas da sua organização.	
O Tag Editor agora é compatível com a descoberta de recursos não marcados	Agora, você pode pesquisar recursos no Tag Editor que não tenham valores de tag aplicados a uma chave de tag específica.	18 de junho de 2019
O console do Tag Editor sai do AWS Systems Manager console	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 Console de gerenciamento da AWS.	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 é compatível com a 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 individuais 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 consistentes 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

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.