AWS Livro branco

Práticas recomendadas para marcação de recursos da AWS

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

Práticas recomendadas para marcação de recursos da AWS: AWS Livro branco

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

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Resumo e introdução i
Você é Well-Architected? 1
Introdução 1
O que são tags? 3
Criar política de tag 8
Definir necessidades e casos de uso 9
Definir e publicar um esquema de marcação 11
AWS Organizations — Políticas de tags 14
ExampleInc-CostAllocation.json 14
ExampleInc-DisasterRecovery.json 15
Implementar e aplicar a marcação 16
Recursos gerenciados manualmente 17
Recursos gerenciados de infraestrutura como código (IaC) 17
CI/CD recursos gerenciados por pipeline 18
Aplicação 20
Medir a eficácia da marcação e promover melhorias 24
Casos de uso das estatísticas 25
Tags para alocação de custos e gerenciamento financeiro 25
Tags de alocação de custos 26
Criar uma estratégia de alocação de custos 27
Tags para operações e suporte 31
Automação de infraestrutura 32
Ciclo de vida da workload 33
Gerenciamento de incidentes 35
Aplicação de patches 36
Observabilidade operacional. 38
Tags para segurança de dados, gerenciamento de riscos e controle de acesso 39
Segurança de dados e gerenciamento de riscos 39
Tags para gerenciamento de identidade e controle de acesso 41
Conclusão 43
Colaboradores 44
Outras fontes de leitura 45
Revisões do documento 47
Avisos 49

AWS Glossário 50
..... li

Práticas recomendadas para marcação de recursos da AWS

Data de publicação: 30 de março de 2023 (Revisões do documento)

A Amazon Web Services (AWS) permite que você atribua metadados a muitos de seus AWS recursos na forma de tags. Cada tag é um rótulo simples composto por uma chave e um valor opcional para armazenar informações sobre o recurso ou dados retidos nesse recurso. Este whitepaper se concentra em marcar casos de uso, estratégias, técnicas e ferramentas que permitem categorizar os recursos por finalidade, equipe, ambiente ou outros critérios relevantes para sua empresa. A implementação de uma estratégia de marcação consistente pode facilitar a filtragem e a pesquisa de recursos, o monitoramento de custos e o uso e o gerenciamento de seu AWS ambiente.

Este artigo se baseia nas práticas e orientações fornecidas no whitepaper Organizando seu AWS ambiente usando várias contas. É recomendável que você leia esse whitepaper antes deste. AWS recomenda que você estabeleça sua base de nuvem de forma holística. Para obter informações adicionais, consulte Establishing your Cloud Foundation on AWS.

Você é Well-Architected?

O Well-Architected Framework da AWS ajuda você a entender os prós e os contras das decisões que você toma ao criar sistemas na nuvem. Os seis pilares do framework permitem a você conhecer as melhores práticas de arquitetura para criar e operar sistemas confiáveis, seguros, econômicos e sustentáveis na nuvem. Usando o AWS Well-Architected Tool, disponível gratuitamente no Console de gerenciamento da AWS, você pode analisar suas workloads em relação a essas práticas recomendadas respondendo a um conjunto de perguntas para cada pilar.

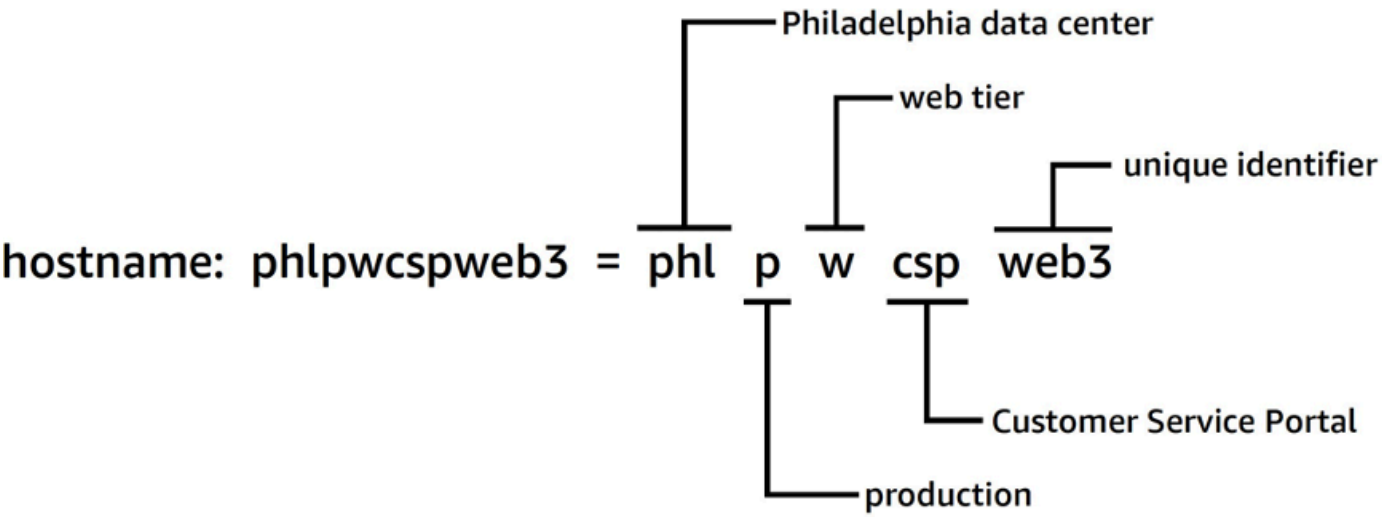
Para obter orientações especializadas e melhores práticas adicionais para a arquitetura de sua nuvem (implantações de arquitetura de referência, diagramas e whitepapers), consulte o Centro de arquitetura da AWS.

Introdução

AWS facilita a implantação de suas cargas de trabalho AWS criando recursos, como instâncias do Amazon EC2, volumes do Amazon EBS, grupos de segurança e funções.AWS Lambda Você também pode escalar e aumentar a frota de AWS recursos que hospeda seus aplicativos, armazena seus dados e expande sua AWS infraestrutura ao longo do tempo. À medida que seu AWS uso aumenta para vários tipos de recursos abrangendo vários aplicativos, você precisará de um

mecanismo para rastrear quais recursos estão atribuídos a cada aplicativo. Use esse mecanismo para apoiar suas atividades operacionais, como monitoramento de custos, gerenciamento de incidentes, aplicação de patches, backup e controle de acesso.

Em ambientes on-premises, esse conhecimento geralmente é capturado em sistemas de gerenciamento de conhecimento, sistemas de gerenciamento de documentos e em páginas wiki internas. Com um banco de dados de gerenciamento de configuração (CMDB), você pode armazenar e gerenciar os metadados detalhados relevantes usando processos padrão de controle de alterações. Essa abordagem fornece governança, mas requer um esforço adicional para ser desenvolvida e mantida. Você pode adotar uma abordagem estruturada para nomear recursos, mas um nome de recurso só pode conter uma quantidade limitada de informações.



Abordagem estruturada para nomeação de recursos

Por exemplo, as instâncias do EC2 têm uma tag predefinida chamada Name, que fornece funcionalidade semelhante e permite nomear workloads à medida que elas são movidas para a AWS.

Em 2010, AWS lançou tags de recursos para fornecer um mecanismo flexível e escalável para anexar metadados aos seus recursos. Este whitepaper orienta você no processo de desenvolvimento e implementação de uma estratégia robusta de marcação em todo o seu ambiente. AWS Essa orientação ajudará você a garantir a consistência e a cobertura da marcação que apoie suas atividades operacionais e de tomada de decisão.

O que são tags?

Uma tag é um par de chave-valor aplicado a um recurso para armazenar metadados sobre esse recurso. Cada tag é um rótulo que consiste em uma chave e um valor opcional. Atualmente, nem todos os serviços e tipos de recursos oferecem suporte a tags (consulte Services that support the Resource Groups Tagging API). Outros serviços podem oferecer suporte a tags por meio de suas próprias etiquetas APIs. Deve-se observar que as tags não são criptografadas e não devem ser usadas para armazenar dados sigilosos, como informações de identificação pessoal (PII).

As tags que um usuário cria e aplica aos AWS recursos usando a AWS CLI API ou a Console de gerenciamento da AWS são conhecidas como tags definidas pelo usuário. Vários AWS serviços AWS CloudFormation, como o Elastic Beanstalk e o Auto Scaling, atribuem automaticamente tags aos recursos que eles criam e gerenciam. Essas chaves são conhecidas como tags geradas pela AWS e geralmente são prefixadas com `aws`. Esse prefixo não pode ser usado em chaves de tag definidas pelo usuário.

Há requisitos de uso e limites no número de tags definidas pelo usuário que podem ser adicionadas a um AWS recurso. Para obter mais informações, consulte os limites e requisitos de nomenclatura de tags no guia de referência AWS geral. AWS as tags geradas não contam nesses limites de tags definidos pelo usuário.

Tabela 1: Exemplos de chaves e valores de tag definidos pelo usuário

ID da instância	Chave de tag	Valor de etiqueta
`i-01234567abcdef89a`	`CostCenter`	`98765`
	`Stack`	`Test`
i-12345678abcdef90b	`CostCenter`	`98765`
	`Stack`	`Production`

Tabela 2 — Exemplos de tags AWS geradas

AWS Chaves de tag geradas	Lógica
`aws:ec2spot:fleet-request-id`	Identifica a solicitação da Amazon EC2 Spot Instance que iniciou a instância
`aws:cloudformation:stack-name`	Identifica a AWS CloudFormation pilha que criou o recurso
`lambda-console:blueprint`	Identifica o blueprint usado como modelo para uma função AWS Lambda
`elasticbeanstalk:environment-name`	Identifica a aplicação que criou o recurso
`aws:servicecatalog: provisionedProductArn`	O nome do recurso da Amazon (ARN) do produto provisionado
`aws:servicecatalog:productArn`	O ARN do produto a partir do qual o produto provisionado foi lançado

AWS as tags geradas formam um namespace. Por exemplo, em um CloudFormation modelo, você define um conjunto de recursos a serem implantados juntos em um`stack`, onde `stack-name` está um nome descritivo que você atribui para identificá-lo. Se você examinar uma chave como `aws:cloudformation:stack-name`, verá que o namespace usado para definir o escopo do parâmetro usa três elementos: a organização aws, o serviço cloudformation e o parâmetro stack-name.

As tags definidas pelo usuário também podem usar namespaces e é recomendável usar um identificador organizacional como prefixo. Isso ajuda você a identificar rapidamente se uma tag é algo do seu esquema gerenciado ou algo definido por um serviço ou ferramenta que você está usando em seu ambiente.

No whitepaper Establishing Your Cloud Foundation on AWS, recomendamos um conjunto de tags que devem ser implementadas. É muito provável que diferentes empresas tenham diferentes padrões permitidos e listas diferentes para uma determinada tag. Observando o exemplo na Tabela 3:

Tabela 3: Mesma chave de tag, regras de validação de valor diferentes

A empresa	Chave de tag	Validação de valores de tag	Exemplo de valor de tag
Empresa A	`CostCenter`	`5432, 5422, 5499`	`5432`
Empresa B	`CostCenter`	`ABC*`	`ABC123`

Se esses dois esquemas estiverem em organizações separadas, não haverá problema com conflitos de tags. No entanto, se esses dois ambientes se fundirem, os namespaces podem entrar em conflito e a validação se torna mais complexa. Esse cenário pode parecer improvável, mas as empresas são adquiridas ou fundidas, e há outros cenários, como clientes trabalhando com um provedor de serviços gerenciados, editora de jogos ou empresa de capital de risco, em que contas de diferentes organizações fazem parte de uma AWS organização compartilhada. Ao usar o nome da empresa como prefixo para definir um namespace exclusivo, esses desafios podem ser evitados, conforme mostrado na Tabela 4:

Tabela 4: Uso de namespaces em chaves de tag

A empresa	Chave de tag	Validação de valores de tag	Exemplo de valor de tag
Empresa A	`company-a :CostCenter`	`5432, 5422, 5499`	`5432`
Empresa B	`company-b :CostCenter`	`ABC*`	`ABC123`

Em organizações grandes e complexas, onde as empresas são adquiridas e alienadas regularmente, essa situação ocorrerá com mais frequência. À medida que os processos e práticas da nova aquisição são harmonizados em todo o grupo, a situação é resolvida. Ter namespaces distintos ajuda porque o uso das tags mais antigas pode ser relatado e as equipes relevantes podem ser contatadas para adotar o novo esquema. Um namespace também pode ser usado para indicar um escopo ou representar um caso de uso ou uma área de responsabilidade alinhada aos proprietários organizacionais.

Tabela 5: Exemplo de escopo ou escopo de caso de uso nas chaves de tag

Caso de uso	Chave de tag	Lógica	Valores permitidos
Classificação de dados	`example-inc:info-sec:data-classification`	Conjunto definido de classificação de dados para segurança da informação	`sensitive`, `company-confidential`, `customer-identifiable`
Operações	`example-inc:dev-ops:environment`	Implemente o agendamento de ambientes de teste e desenvolvimento	`development`, `staging`, `quality-assurance`, `production`
Recuperação de desastres	`example-inc:disaster-recovery:rpo`	Defina o objetivo de ponto de recuperação (RPO) para um recurso	6h, 24h
Alocação de custos	`example-inc:cost-allocation:business-unit`	As equipes financeiras precisam de relatórios de custos sobre o uso e os gastos de cada equipe	`corporate`, `recruitment`, `support`, `engineering`

As tags são simples e flexíveis. Tanto a chave quanto o valor da tag são cadeias de caracteres de comprimento variável e podem suportar um amplo conjunto de caracteres. Para obter mais informações sobre comprimentos e conjuntos de caracteres, consulte Tagging AWS resources na Referência geral da AWS . As tags diferenciam maiúsculas de minúsculas, o que significa que `costCenter` e `costcenter` são chaves de tag diferentes. Em países diferentes, a grafia de uma palavra pode ser diferente, o que pode afetar suas teclas. Por exemplo, nos Estados Unidos, pode-se definir uma chave como `costcenter`, mas, no Reino Unido, `costcentre` pode ser preferível. Essas são chaves diferentes do ponto de vista da marcação de recursos. Defina ortografia, maiúsculas e minúsculas e pontuação como parte de sua estratégia de marcação. Use essas definições como referência para qualquer pessoa que crie ou gerencie recursos. Esse tópico é discutido em mais detalhes na próxima seção, Criar política de tag.

> **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 detalhes.

Criar política de tag

Como acontece com muitas práticas em operações, a implementação de uma estratégia de marcação é um processo de iteração e aprimoramento. Comece aos poucos, com sua prioridade imediata e aumente o esquema de marcação conforme necessário.

Marcação de iteração estratégica e do ciclo de melhoria

Durante todo esse processo, a propriedade é fundamental para a responsabilidade e o progresso. Como as tags podem ser usadas para diversas finalidades, a estratégia geral de marcação pode ser dividida em áreas de responsabilidade dentro de uma organização. A marcação permite uma abordagem programática de atividades que dependem da caracterização dos recursos. A variedade de partes interessadas que podem se beneficiar da marcação dependerá do tamanho da organização e das práticas operacionais. Organizações maiores podem se beneficiar da definição clara das responsabilidades das equipes envolvidas na criação e implementação de uma estratégia de marcação. Algumas partes interessadas podem ser responsáveis por identificar as necessidades

(definir casos de uso) de marcação; outras podem ser responsáveis por manter, implementar e melhorar a estratégia de marcação.

Ao atribuir a propriedade, você está em uma boa posição para implementar aspectos individuais da estratégia. Quando apropriado, essa propriedade pode ser formalizada como política e documentada em uma matriz de responsabilidade (por exemplo, RACI: Responsável, Responsabilizado, Consultado e Informado) ou em um modelo de responsabilidade compartilhada. Em organizações menores, as equipes podem desempenhar várias funções em uma estratégia de marcação, desde a definição dos requisitos até a implementação e a fiscalização.

Definir necessidades e casos de uso

Comece a criar sua estratégia interagindo com as partes interessadas que têm uma necessidade fundamental subjacente de consumir metadados. Essas equipes definem os metadados com os quais os recursos precisam ser marcados para apoiar suas atividades, como relatórios, automação e classificação de dados. Eles descrevem como os recursos precisam ser organizados e para quais políticas eles precisam ser mapeados. Exemplos de papéis e funções que essas partes interessadas podem ter nas organizações incluem:

- O financeiro e a linha de negócios precisam entender o valor do investimento associando-o aos custos para priorizar as ações que precisam ser executadas ao lidar com a ineficiência. Entender o custo versus o valor gerado ajuda a identificar linhas de negócios ou ofertas de produtos malsucedidas. Isso leva a decisões informadas sobre suporte contínuo, adoção de uma alternativa (por exemplo, uso de uma oferta de SaaS ou serviço gerenciado) ou retirada de uma oferta comercial não lucrativa.
- A governança e a conformidade precisam entender a categorização dos dados (por exemplo, públicos, sigilosos ou confidenciais), se uma workload específica está dentro ou fora do escopo da auditoria em relação a um padrão ou regulamento específico e a importância do serviço (se o serviço ou a aplicação é essencial para os negócios) para aplicar controles e supervisão adequados, como permissões, políticas e monitoramento.
- As operações e o desenvolvimento precisam entender o ciclo de vida da workload, os estágios implementados de seus produtos compatíveis e o gerenciamento dos estágios de lançamento (por exemplo, desenvolvimento, teste, divisão de produção) e suas priorizações de suporte associadas e requisitos de gerenciamento de partes interessadas. Deveres como backups, aplicação de patches, observabilidade e suspensão de uso também precisam ser definidos e compreendidos.

- A Segurança da Informação (InfoSec) e as Operações de Segurança (SecOps) descrevem quais controles devem ser aplicados e quais são recomendados. InfoSec normalmente define a implementação dos controles e geralmente SecOps é responsável por gerenciar esses controles.

Dependendo do seu caso de uso, das prioridades, do tamanho da sua organização e das práticas operacionais, você pode precisar da representação de várias equipes dentro da organização, como finanças (incluindo compras), segurança da informação, capacitação da nuvem e operações na nuvem. Você também precisa da representação dos proprietários de aplicações e processos para funções como aplicação de patches, backup e restauração, monitoramento, agendamento de tarefas e recuperação de desastres. Esses representantes ajudam a orientar a definição, a implementação e a medir a eficácia da estratégia de marcação. Eles devem trabalhar de trás para frente com as partes interessadas e seus casos de uso e conduzir um workshop multifuncional. No workshop, eles têm a chance de compartilhar suas perspectivas e necessidades e ajudar a impulsionar uma estratégia geral. Exemplos de participantes e seu envolvimento em vários casos de uso são descritos posteriormente neste whitepaper.

As partes interessadas também definem e validam as chaves para as tags obrigatórias e podem recomendar o escopo das tags opcionais. Por exemplo, as equipes financeiras podem precisar relacionar um recurso a um centro de custos interno, a uma unidade de negócios ou a ambos. Assim, eles podem exigir que certas chaves de tag, como `CostCenter` e`BusinessUnit`, sejam tornadas obrigatórias. As equipes de desenvolvimento individuais podem decidir usar tags adicionais para fins de automação, como `EnvironmentName`, `OptIn` ou `OptOut`.

As principais partes interessadas precisam concordar com a abordagem da estratégia de marcação e documentar as respostas para questões relacionadas à conformidade e à governança, como:

- Quais casos de uso precisam ser abordados?
- Quem é responsável por marcar recursos (implementação)?
- Como as tags são aplicadas e quais métodos e automação serão usados (proativos ou reativos)?
- Como a eficácia e as metas da marcação são medidas?
- Com que frequência a estratégia de marcação deve ser revisada?
- Quem impulsiona as melhorias? Como isso é feito?

Funções de negócios, como capacitação de nuvem, escritório de negócios em nuvem e engenharia de plataforma em nuvem, podem então desempenhar o papel de facilitadoras do processo de

criação da estratégia de marcação, ajudar a impulsionar sua adoção e garantir a consistência de sua aplicação medindo o progresso, removendo obstáculos e reduzindo o esforço duplicado.

Definir e publicar um esquema de marcação

Use uma abordagem consistente para marcar seus AWS recursos, tanto para tags obrigatórias quanto opcionais. Um esquema abrangente de marcação ajuda você a alcançar essa consistência. Os exemplos a seguir podem ajudá-lo a começar:

- Concorde com as chaves de tag obrigatórias
- Defina valores aceitáveis e convenções de nomenclatura de tags (letras maiúsculas ou minúsculas, traços ou sublinhados, hierarquia etc.)
- Confirmar que os valores não constituiriam informações de identificação pessoal (PII)
- Decidir quem pode definir e criar novas chaves de tag
- Chegue a um acordo sobre como adicionar novos valores de tag obrigatórios e como gerenciar tags opcionais

Analise a tabela de categorias de marcação a seguir, que pode ser usada como base do que você pode incluir em seu esquema de marcação. Você ainda precisa determinar a convenção que usará para a chave da tag e quais valores são permitidos para cada uma. O esquema de marcação é o documento no qual você define isso para seu ambiente.

Tabela 6: Exemplo de um esquema de marcação definitivo (parte 1)

Caso de uso	Chave de tag	Lógica	Valores permitidos (listados ou valor prefix/sux)	Usado para alocação de custos	Tipos de recursos	Escopo	Obrigatório
Alocação de custos	`example-inc:cost-allocation: ApplicationId`	Acompanhe o custo versus o valor gerado por cada linha de negócios	`DataLakeX` , `RetailSiteX`	S	Todos	Todos	Obrigatório
Alocação de custos	`example-inc:cost-allocation: BusinessUnitId`	Monitore os custos por unidade de negócios	`Architecture` , `DevOps`, `Finance`	S	Todos	Todos	Obrigatório
Alocação de custos	`example-inc:cost-allocation: CostCenter`	Monitore os custos por centro de custo	`123-*`	S	Todos	Todos	Obrigatório
Alocação de custos	`example-inc:cost-allocation :Owner`	Qual detentor do orçamento é responsável por essa workload	`Marketing` , `RetailSupport`	S	Todos	Todos	Obrigatório
Controle de acesso	`example-inc:access-control: LayerId`	Identifique SubComponent /Layer para conceder	`DB_Layer`, `Web_Layer` , `App_Layer`	N	Todos	Todos	Opcional

Tabela 6: Exemplo de um esquema de marcação definitivo (parte 2)

Caso de uso	Chave de tag	Lógica	Valores permitidos (listados ou valor prefix/sux)	Usado para alocação de custos	Tipos de recursos	Escopo	Obrigatório
DevOps	`example-inc:operations: Owner`	Que team/squad é responsável pela criação e manutenção do recurso	`Squad01`	N	Todos	Todos	Obrigatório
Recuperação de desastres	`example-inc:disaster-recovery:rpo`	Defina o objetivo de ponto de recuperação (RPO) para um recurso	`6h`, `24h`	N	S3, EBS	Prod	Obrigatório
Classificação de dados	`example-inc:data: classification`	Classifique os dados para fins de conformidade e governança	`Public`, `Private`, `Confidential` , `Restricted`	N	S3, EBS	Todos	Obrigatório
Compliance	`example-inc:compliance: framework`	Identifica a estrutura de conformidade à qual a workload está sujeita	`PCI-DSS`, `HIPAA`	N	Todos	Prod	Obrigatório

Depois que o esquema de marcação for definido, gerencie o esquema em um repositório com controle de versão que seja acessível a todas as partes interessadas relevantes para facilitar a consulta e as atualizações rastreáveis. Essa abordagem melhora a eficiência e permite agilidade.

AWS Organizations — Políticas de tags

As políticas AWS Organizations permitem que você aplique tipos adicionais de governança Contas da AWS em sua organização. Uma política de tags é como você pode expressar seu esquema de marcação no formato JSON para que a plataforma possa relatar e, opcionalmente, aplicar o esquema em seu ambiente. AWS A política de tags define os valores que são aceitáveis para uma chave de tag em tipos de recursos específicos. Essa política pode ter a forma de uma lista de valores ou de um prefixo seguido por um caractere curinga (*). A abordagem de prefixo simples é menos rigorosa do que uma lista discreta de valores, mas requer menos manutenção.

Os exemplos a seguir mostram como definir uma política de marcação para validar os valores que são aceitáveis para uma determinada chave. Trabalhando com a definição tabular amigável do esquema, você pode transcrever essas informações em uma ou mais políticas de tag. Políticas separadas podem ser usadas para apoiar a propriedade delegada ou algumas políticas podem ser aplicadas somente em cenários específicos.

ExampleInc-CostAllocation.json

A seguir, um exemplo de política de tag que informa sobre tags de alocação de custos:

```
{
  "tags": {
    "example-inc:cost-allocation:ApplicationId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:ApplicationId"
      },
      "tag_value": {
        "@@assign": [
          "DataLakeX",
          "RetailSiteX"
        ]
      }
    },
    "example-inc:cost-allocation:BusinessUnitId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:BusinessUnitId"
      },
```

```
      "tag_value": {
        "@@assign": [
          "Architecture",
          "DevOps",
          "FinanceDataLakeX"
        ]
      }
    },
    "example-inc:cost-allocation:CostCenter": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "123-*"
        ]
      }
    }
  }
}
```

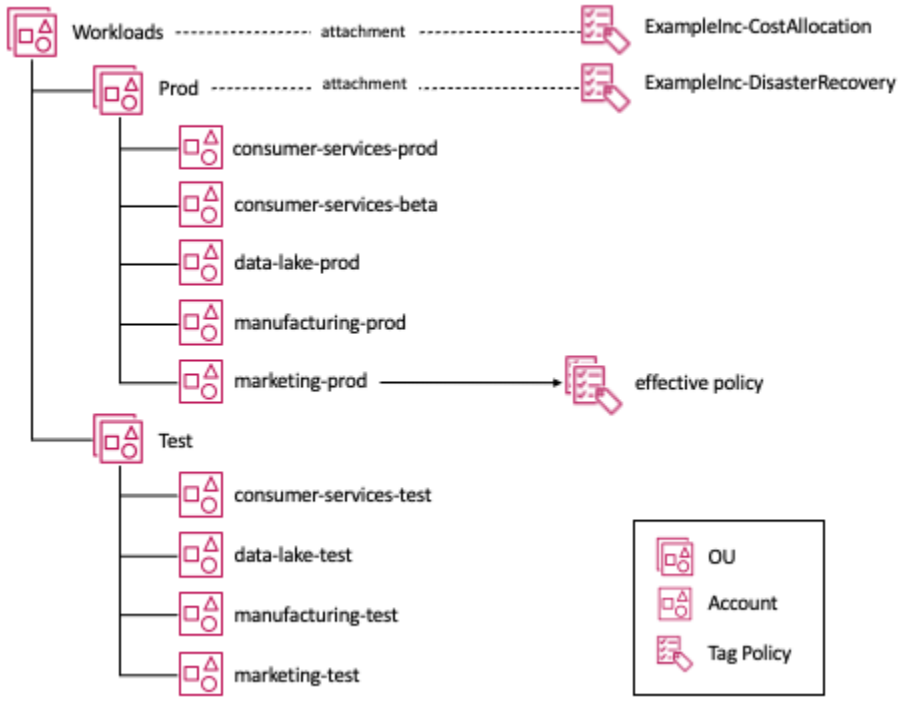
ExampleInc-DisasterRecovery.json

Veja a seguir um exemplo de uma política de tags que relata as tags de recuperação de desastres.

```
{
    "tags": {
        "example-inc:disaster-recovery:rpo": {
            "tag_key": {
                "@@assign": "example-inc:disaster-recovery:rpo"
            },
            "tag_value": {
                "@@assign": [
                    "6h",
                    "24h"
                ]
            }
        }
    }
}
```

Neste exemplo, a política de tag `ExampleInc-CostAllocation` está anexada à UO `Workloads` e, portanto, aplica-se a todas as contas nas UOs filhas `Prod` e `Test`. Da mesma forma, a política

de tag `ExampleInc-DisasterRecovery` é anexada à UO `Prod` e, portanto, aplica-se somente a contas abaixo dessa UO. O whitepaper Organizing Your Environment Using Multiple Accounts explora as estruturas de UO recomendadas com mais detalhes.



Anexação de políticas de tag a uma estrutura de UO

Observando a conta `marketing-prod` no diagrama, as duas políticas de tag se aplicam a essa conta, então temos o conceito de uma política efetiva, que é a convolução das políticas de um determinado tipo que se aplicam a uma conta. Se você gerencia principalmente seus recursos manualmente, pode revisar a política efetiva visitando as Editor:Tag políticas de Resource Groups & Tag no console. Se você usa infraestrutura como código (IaC) ou scripts para gerenciar seus recursos, você pode usar a chamada de API `AWS::Organizations::DescribeEffectivePolicy`.

Implementar e aplicar a marcação

Nesta seção, apresentaremos as ferramentas disponíveis para as seguintes estratégias de gerenciamento de recursos: manual, infraestrutura como código (IaC) e integration/continuous entrega contínua (CI/CD). A principal dimensão dessas abordagens é uma taxa de implantação cada vez mais frequente.

Recursos gerenciados manualmente

Normalmente, essas workloads se enquadram nos estágios básicos ou de migração da adoção. Geralmente, essas são cargas de trabalho simples, em grande parte estáticas, que foram criadas usando procedimentos escritos tradicionais ou migradas como estão usando ferramentas, como AWS Transform MGN de um ambiente local. Ferramentas de migração, como o Migration Hub e o MGN, podem aplicar tags como parte do processo de migração. No entanto, se as tags não foram aplicadas durante a migração original ou o esquema de marcação mudou desde então, o Editor de tags (um recurso do Console de gerenciamento da AWS) permite pesquisar recursos usando uma variedade de critérios de pesquisa e adicionar, modificar ou excluir tags em massa. Os critérios de pesquisa podem incluir recursos com ou sem a presença de uma tag ou valor específico. A API AWS Resource Tagging permite que você execute essas funções programaticamente.

À medida que essas workloads são modernizadas, tipos de recursos, como grupos do Auto Scaling, são introduzidos. Esses tipos de recurso permitem maior elasticidade e maior resiliência. O grupo do Auto Scaling gerencia as instâncias do Amazon EC2 em seu nome, no entanto, você ainda pode querer que as instâncias do EC2 sejam marcadas de forma consistente com os recursos criados manualmente. Um modelo de lançamento do Amazon EC2 fornece os meios para especificar as tags que o Auto Scaling deve aplicar às instâncias que ele cria.

Quando os recursos de uma workload estão sendo gerenciados manualmente, pode ser útil automatizar a marcação de recursos. Há várias soluções disponíveis. Uma abordagem é usar Regras do AWS Config, que pode verificar `required_tags` e iniciar uma função Lambda para aplicá-las. Regras do AWS Config será descrito com mais detalhes posteriormente neste whitepaper.

Recursos gerenciados de infraestrutura como código (IaC)

AWS CloudFormation fornece uma linguagem comum para provisionar todos os recursos de infraestrutura em seu AWS ambiente. CloudFormation modelos são arquivos JSON ou YAML que criam AWS recursos de forma automatizada. Ao criar AWS recursos usando CloudFormation modelos, você pode usar a propriedade CloudFormation Resource Tags para aplicar tags aos tipos de recursos compatíveis após a criação. Gerenciar as tags e os recursos com o IaC ajuda a garantir a consistência.

Quando os recursos são criados por AWS CloudFormation, o serviço aplica automaticamente um conjunto de tags AWS definidas aos recursos criados pelo AWS CloudFormation modelo. Eles são:

```
aws:cloudformation:stack-name
aws:cloudformation:stack-id
```

```
aws:cloudformation:logical-id
```

Você pode definir facilmente um grupo de recursos com base na AWS CloudFormation pilha. Essas tags da AWS definidas são herdadas pelos recursos criados pela pilha. No entanto, para instâncias do Amazon EC2 dentro de um grupo de Auto Scaling, `AWS::AutoScaling::AutoScalingGroup TagProperty`as necessidades devem ser definidas na definição do grupo Auto Scaling em seu modelo. AWS CloudFormation Como alternativa, se você estiver usando um modelo de inicialização do EC2 com o grupo do Auto Scaling, poderá definir as tags em sua definição. É recomendável usar modelos de inicialização do EC2 com grupos de Auto Scaling ou com AWS um serviço de contêiner. Esses serviços podem ajudar a garantir a marcação consistente de suas instâncias do Amazon EC2 e também oferecer suporte ao Auto Scaling em vários tipos de instância e opções de compra, o que pode melhorar a resiliência e otimizar seus custos computacionais.

AWS CloudFormation Os ganchos fornecem aos desenvolvedores um meio de manter os principais aspectos de seus aplicativos consistentes com os padrões da organização. Os hooks podem ser configurados para fornecer um aviso ou impedir a implantação. Esse recurso é mais adequado para verificar os principais elementos de configuração em seus modelos, como se um grupo do Auto Scaling está configurado para aplicar tags definidas pelo cliente a todas as instâncias do Amazon EC2 que ele executa ou para garantir que todos os buckets do Amazon S3 sejam criados com as configurações de criptografia necessárias. Em ambos os casos, a avaliação dessa conformidade está sendo adiada para o início do processo de implantação com AWS CloudFormation ganchos antes da implantação.

AWS CloudFormation fornece a capacidade de detectar quando um recurso (consulte Recursos que oferecem suporte à detecção de desvios) provisionado a partir de um modelo foi modificado e os recursos não correspondem mais às configurações de modelo esperadas. Isso é conhecido como deriva. Se você usa a automação para aplicar tags aos recursos gerenciados via IaC, então você os está modificando, introduzindo o drift. Ao usar o IaC, atualmente é recomendável gerenciar quaisquer requisitos de marcação como parte dos modelos do IaC, implementar AWS CloudFormation ganchos e publicar conjuntos de regras do AWS CloudFormation Guard que possam ser usados pela automação.

CI/CD recursos gerenciados por pipeline

À medida que a maturidade de uma carga de trabalho aumenta, é provável que técnicas como integração contínua e implantação contínua (CI/CD) sejam adotadas. Essas técnicas ajudam a reduzir o risco de implantação, facilitando a implantação de pequenas alterações com mais frequência com o aumento da automação dos testes. Uma estratégia de observabilidade que detecta

um comportamento inesperado introduzido por uma implantação pode reverter automaticamente a implantação com o mínimo impacto no usuário. Quando você chega ao estágio de implementar dezenas de vezes por dia, aplicar tags retroativamente simplesmente não é mais prático. Tudo precisa ser expresso como código ou configuração, ter controle de versão e, sempre que possível, ser testado e avaliado antes da implantação na produção. No modelo combinado de desenvolvimento e operações (DevOps), muitas das práticas abordam as considerações operacionais como código e as validam no início do ciclo de vida da implantação.

O ideal é realizar essas verificações o mais cedo possível no processo (conforme mostrado com AWS CloudFormation ganchos), para ter certeza de que seu AWS CloudFormation modelo atende às suas políticas antes que elas saiam da máquina do desenvolvedor.

AWS CloudFormation O Guard 2.0 fornece os meios para escrever regras preventivas de conformidade para qualquer coisa que você possa definir. CloudFormation O modelo é validado de acordo com as regras do ambiente de desenvolvimento. Claramente, esse recurso tem uma variedade de aplicações, mas neste whitepaper, veremos apenas alguns exemplos que garantiriam que ele estivesse sempre `AWS::AutoScaling::AutoScalingGroup TagProperty`sendo usado.

Veja a seguir um exemplo de uma regra do CloudFormation Guard:

```
let all_asgs = Resources.*[ Type == 'AWS::AutoScaling::AutoScalingGroup' ]

rule tags_asg_automation_EnvironmentId when %all_asgs !empty {
    let required_tags = %all_asgs.Properties.Tags.*[
        Key == 'example-inc:automation:EnvironmentId' ]
    %required_tags[*] {
        PropagateAtLaunch == 'true'
        Value IN ['Prod', 'Dev', 'Test', 'Sandbox']
        <<Tag must have a permitted value
          Tag must have PropagateAtLaunch set to 'true'>>
    }
}

rule tags_asg_costAllocation_CostCenter when %all_asgs !empty {
    let required_tags = %all_asgs.Properties.Tags.*[
        Key == 'example-inc:cost-allocation:CostCenter' ]
    %required_tags[*] {
        PropagateAtLaunch == 'true'
        Value == /^123-/
        <<Tag must have a permitted value
          Tag must have PropagateAtLaunch set to 'true'>>
    }
```

```
}
```

No exemplo de código, filtramos o modelo para todos os recursos que são do tipo `AutoScalingGroup` e, em seguida, temos duas regras:

- **`tags_asg_automation_EnvironmentId`**: verifica se existe uma tag com essa chave, se ela tem um valor dentro da lista de valores permitidos e se `PropagateAtLaunch` está definido como `true`.
- **`tags_asg_costAllocation_CostCenter`**: verifica se existe uma tag com essa chave, se ela tem um valor que começa com o valor de prefixo definido e se `PropagateAtLaunch` está definido como `true`.

Aplicação

Conforme descrito anteriormente, oResource Groups & Tag Editor fornece os meios para identificar onde seus recursos não atendem aos requisitos de marcação definidos nas políticas de tags aplicadas às OUs da organização. O acesso à ferramenta do console do Resource Groups & Tag Editor de dentro da conta de um membro da organização mostra as políticas que se aplicam a essa conta e os recursos dentro da conta que não atendem aos requisitos da política de tags. Se acessado a partir da conta de gerenciamento (e se as políticas de tags tiverem o acesso habilitado nos serviços em AWS Organizations), é possível visualizar a conformidade da política de tags para todas as contas vinculadas na organização.

Na própria Política de Tags, você pode ativar a aplicação de tipos de recursos específicos. No exemplo de política a seguir, adicionamos a imposição de que todos os recursos dos tipos `ec2:instance` e `ec2:volume` devem estar em conformidade com a política. Há algumas limitações conhecidas, como a necessidade de haver uma tag em um recurso para que ele seja avaliado pela política de tags. Consulte Recursos que apoiam a fiscalização com políticas de tags para obter uma lista.

ExampleInc-Cost-Allocation.json

Veja a seguir um exemplo de uma política de tags em que os relatórios and/or impõem tags de alocação de custos:

```
{
  "tags": {
    "example-inc:cost-allocation:ApplicationId": {
      "tag_key": {
```

```
        "@@assign": "example-inc:cost-allocation:ApplicationId"
      },
      "tag_value": {
        "@@assign": [
          "DataLakeX",
          "RetailSiteX"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "ec2:instance",
          "ec2:volume"
        ]
      }
    },
    "example-inc:cost-allocation:BusinessUnitId": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:BusinessUnitId"
      },
      "tag_value": {
        "@@assign": [
          "Architecture",
          "DevOps",
          "FinanceDataLakeX"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "ec2:instance",
          "ec2:volume"
        ]
      }
    },
    "example-inc:cost-allocation:CostCenter": {
      "tag_key": {
        "@@assign": "example-inc:cost-allocation:CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "123-*"
        ]
      },
      "enforced_for": {
        "@@assign": [
```

```
          "ec2:instance",
          "ec2:volume"
        ]
      }
    }
  }
}
```

AWS Config (**`required_tag`**)

AWS Config é um serviço que permite avaliar, auditar e avaliar as configurações de seus AWS recursos (consulte Tipos de recursos suportados por AWS Config). No caso da marcação, podemos usá-la para identificar recursos que não têm tags com chaves específicas, usando a regra `required_tags` (consulte Resource types supported by required_tags). No exemplo anterior, podemos testar a existência da chave em todas as instâncias do Amazon EC2. Nos casos em que a chave não existir, a instância será registrada como não compatível. Este AWS CloudFormation modelo descreve uma AWS Config regra para testar a presença das chaves obrigatórias descritas na tabela, nos buckets do Amazon S3, nas instâncias do Amazon EC2 e nos volumes do Amazon EBS.

```
Resources:
 MandatoryTags:
   Type: AWS::Config::ConfigRule
   Properties:
     ConfigRuleName: ExampleIncMandatoryTags
     Description: These tags should be in place
     InputParameters:
       tag1Key: example-inc:cost-allocation:ApplicationId
       tag2Key: example-inc:cost-allocation:BusinessUnitId
       tag3Key: example-inc:cost-allocation:CostCenter
       tag4Key: example-inc:automation:EnvironmentId
     Scope:
       ComplianceResourceTypes:
       - "AWS::S3::Bucket"
       - "AWS::EC2::Instance"
       - "AWS::EC2::Volume"
     Source:
       Owner: AWS
SourceIdentifier: REQUIRED_TAGS
```

Para ambientes em que os recursos são gerenciados manualmente, uma AWS Config regra pode ser aprimorada para adicionar automaticamente a chave de tag ausente aos recursos usando uma

correção automatizada por meio de uma AWS Lambda função. Embora isso funcione bem para workloads estáticas, é progressivamente menos eficaz à medida que você começa a gerenciar seus recursos por meio de IaC e pipelines de implantação.

AWS Organizations — As políticas de controle de serviços (SCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões em sua organização. As SCPs oferecem controle central sobre as permissões máximas disponíveis para todas as contas da sua organização ou unidade organizacional (UO). As SCPs afetam apenas os usuários e as funções gerenciados por contas que fazem parte da organização. Embora não afetem os recursos diretamente, eles restringem as permissões de usuários e funções, o que inclui as permissões para marcar ações. Com relação à marcação, os SCPs podem fornecer granularidade adicional para a aplicação de tags, além do que as políticas de tags podem fornecer.

No exemplo a seguir, a política negará solicitações `ec2:RunInstances` quando a tag `example-inc:cost-allocation:CostCenter` não estiver presente.

O seguinte é uma negação do SCP:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/example-inc:cost-allocation:CostCenter": "true"
        }
      }
    }
  ]
}
```

Não é possível recuperar a política efetiva de controle de serviços que se aplica a uma conta vinculada por design. Quando você impõe a marcação com SCPs, a documentação precisa estar disponível para os desenvolvedores para que eles possam garantir que seus recursos atendam às políticas que foram aplicadas às suas contas. Fornecer acesso somente de leitura aos CloudTrail eventos em sua conta pode ajudar os desenvolvedores na tarefa de depuração quando seus recursos não estão em conformidade.

Medir a eficácia da marcação e promover melhorias

Depois de implementar uma estratégia de marcação, é importante medir sua eficácia em relação aos casos de uso desejados. A medida de eficácia variará de acordo com o caso de uso. Por exemplo:

- Atribuição de custos: você pode medir a cobertura de marcação de recursos com base nos gastos usando ferramentas como o AWS Cost Explorer ou o Relatório de Custos e Uso da AWS. Por exemplo, você pode monitorar a porcentagem de recursos marcados ou não marcados que geram cobranças, especialmente monitorando chaves de tag específicas.
- Automação: talvez você queira auditar se o resultado desejado foi alcançado. Por exemplo, se as instâncias não produtivas do Amazon EC2 são suspensas fora do horário comercial, auditando os horários de início e término da instância.

O Resource Groups & Tag Editor na conta de gerenciamento fornece recursos adicionais para analisar a conformidade com a política de tags para todas as contas vinculadas em sua organização.

Com base nos resultados da medição da eficácia da marcação, identifique se são necessárias melhorias ou alterações em alguma das etapas, como definição do caso de uso, implementação ou aplicação do esquema de marcação. Faça as alterações necessárias e repita o ciclo até que a eficácia desejada seja alcançada. No exemplo com atribuição de custos, você pode observar a melhoria percentual.

Como são os desenvolvedores e operadores que precisam realizar a marcação real dos recursos, é fundamental que eles assumam a responsabilidade. Essa não é a única responsabilidade adicional que as equipes normalmente assumem em sua jornada de AWS adoção. O aumento da responsabilidade pela segurança e pelo custo de desenvolvimento e operação das aplicações também é importante. As organizações costumam usar metas e metas como meio de motivar a adoção de novas práticas, então isso também pode ser aplicado aqui.

Casos de uso das estatísticas

Tópicos

- Tags para alocação de custos e gerenciamento financeiro
- Tags para operações e suporte
- Tags para segurança de dados, gerenciamento de riscos e controle de acesso

Tags para alocação de custos e gerenciamento financeiro

Um dos primeiros casos de uso de tags que as organizações costumam abordar é a visibilidade e o gerenciamento de custos e uso. Geralmente, existem alguns motivos para isso:

- Normalmente, é um cenário bem compreendido e os requisitos são bem conhecidos. Por exemplo, as equipes financeiras querem ver o custo total das workloads e da infraestrutura que abrangem vários serviços, recursos, contas ou equipes. Uma forma de obter essa visibilidade de custos é por meio da marcação consistente dos recursos.
- As tags e seus valores estão claramente definidos. Normalmente, mecanismos de alocação de custos já existem nos sistemas financeiros de uma organização, por exemplo, rastreamento por centro de custo, unidade de negócios, equipe ou função da organização.
- Retorno do investimento rápido e demonstrável. É possível acompanhar as tendências de otimização de custos ao longo do tempo quando os recursos são marcados de forma consistente, por exemplo, para recursos que foram devidamente dimensionados, escalados automaticamente ou programados.

Entender como você incorre em custos AWS permite que você tome decisões financeiras informadas. Saber onde você incorreu em custos no nível de recursos, workload, equipe ou organização melhora sua compreensão do valor entregue no nível aplicável quando comparado aos resultados comerciais alcançados.

As equipes de engenharia podem não ter experiência com o gerenciamento financeiro de seus recursos. Contratar uma pessoa com uma habilidade especializada em gestão AWS financeira que possa treinar equipes de engenharia e desenvolvimento nos fundamentos da gestão AWS financeira e criar um relacionamento entre finanças e engenharia para promover a cultura FinOps ajudará a alcançar resultados mensuráveis para a empresa e incentivará as equipes a construir pensando nos custos. O estabelecimento de boas práticas financeiras é abordado em profundidade pelo Pilar

Otimização de custos do Well-Architected Framework, mas abordaremos alguns dos princípios fundamentais neste whitepaper.

Tags de alocação de custos

A alocação de custos se refere à atribuição ou distribuição dos custos incorridos aos usuários ou beneficiários desses custos após um processo definido. No contexto deste whitepaper, dividimos a alocação de custos em dois tipos: showback e estorno.

As ferramentas e os mecanismos de showback contribuem para o reconhecimento de custos. O estorno ajuda na recuperação de custos e promove o reconhecimento de custos. O showback refere-se à apresentação, ao cálculo e à geração de relatórios de cobranças incorridas por uma entidade específica, como unidade de negócios, aplicação, usuário ou centro de custos. Por exemplo: “a equipe de engenharia de infraestrutura foi responsável por $ X de gastos com a AWS no mês passado”. O estorno se refere à cobrança real dos custos incorridos a essas entidades por meio dos processos contábeis internos de uma organização, como sistemas financeiros ou vales diários. Por exemplo: “$ X foi deduzido do orçamento da equipe de engenharia de infraestrutura” AWS .
Em ambos os casos, marcar recursos de forma adequada pode ajudar a alocar o custo para uma entidade, com a única diferença sendo se existe a expectativa de que alguém efetuará ou não um pagamento.

A governança financeira da sua organização pode exigir uma contabilidade transparente dos custos incorridos no nível da aplicação, da unidade de negócios, do centro de custos e da equipe. A execução de atribuição de custos possibilitada pelas tags de alocação de custos fornece os dados necessários para atribuir com precisão os custos incorridos por uma entidade a partir de recursos devidamente marcados.

- Responsabilidade: garanta que o custo seja alocado aos responsáveis pelo uso dos recursos. Um único ponto de serviço ou grupo pode ser responsável pelas análises e relatórios de gastos.
- Transparência financeira: mostre uma visualização clara das alocações de caixa à TI criando painéis eficazes e análises de custos significativas para a liderança.
- Investimentos respaldados em TI: acompanhe o ROI com base no projeto, aplicação ou linha de negócios e capacite as equipes a tomarem melhores decisões de negócios, por exemplo, alocando mais fundos a aplicações que geram receita.

Em resumo, as tags de alocação de custos podem ajudar a dizer a você:

- Quem é o dono dos gastos e é responsável por otimizá-los?

- Qual workload, aplicação ou produto está incorrendo nos gastos? Qual ambiente ou estágio?
- Quais áreas de gastos estão crescendo mais rápido?
- Quanto gasto pode ser deduzido de um AWS orçamento com base nas tendências passadas?
- Qual foi o impacto dos esforços de otimização de custos em workloads, aplicações ou produtos específicos?

A ativação de etiquetas de recursos para alocação de custos ajuda na definição de práticas de medição dentro da organização que podem ser usadas para fornecer a visibilidade do AWS uso que aumenta a transparência na responsabilidade pelos gastos. Também se concentra em criar um nível adequado de granularidade com relação à visibilidade de custos e uso e influenciar os comportamentos de consumo da nuvem por meio de relatórios de alocação de custos e rastreamento de KPI.

Criar uma estratégia de alocação de custos

Definir e implementar um modelo de alocação de custos

Crie uma estrutura de contas e custos para os recursos que estão sendo implantados AWS. Estabeleça a relação entre os custos dos AWS gastos, como esses custos foram incorridos e quem ou o que incorreu nesses custos. As estruturas de custo comuns são baseadas em AWS Organizations Contas da AWS,, ambientes e entidades dentro de suas organizações, como uma linha de negócios ou carga de trabalho. As estruturas de custos podem se basear em vários atributos para permitir o exame dos custos de maneiras distintas ou em diferentes níveis de detalhamento, como transferir os custos de workloads individuais para a linha de negócios a que atendem.

Ao escolher uma estrutura de custos que se alinhe aos resultados desejados, avalie os mecanismos de alocação de custos quanto à facilidade de implementação versus a precisão desejada. Isso pode incluir considerações em relação à responsabilidade, disponibilidade de ferramentas e mudanças culturais. Três modelos populares de alocação de custos com os quais AWS os clientes geralmente partem são:

- Baseado em contas — Esse modelo exige o mínimo de esforço e fornece alta precisão para devoluções e cobranças, além de ser adequado para organizações que têm uma estrutura de contas definida (e é consistente com as recomendações do whitepaper Organizando seu AWS ambiente usando várias contas). Isso fornece uma visibilidade clara dos custos por conta. Para visibilidade e alocação de custos, você pode usar o AWS Cost Explorer, o Relatório de Custos e Uso da https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-managing-

costs.html, bem como o AWS Budgets para monitoramento e rastreamento de custos. Essas ferramentas fornecem opções de filtragem e agrupamento por. Contas da AWS Do ponto de vista da alocação de custos, esse modelo não precisa depender da marcação precisa de recursos individuais.

- Baseado em unidade de negócios ou em equipe: custo alocável para equipes, unidades de negócios ou organizações dentro de uma empresa. Esse modelo exige um esforço moderado, fornece alta precisão para showbacks e estornos e é adequado para organizações que definiram um estrutura de conta (normalmente usando o AWS Organizations), com separação entre várias equipes, aplicações e tipos de workload. Isso fornece uma visibilidade clara dos custos entre equipes e aplicações e, como benefício adicional, reduz o risco de atingir as cotas de serviço da AWS em uma única Conta da AWS. Por exemplo, cada equipe pode ter cinco contas (`prod`, `staging`, `test`, `dev`, `sandbox`) e duas equipes e aplicações não compartilharão a mesma conta. Com essa estrutura, o Categorias de Custos da AWS fornecerá a funcionalidade de agrupar contas ou outras tags (“metamarcação”) em categorias, que podem ser rastreadas nas ferramentas mencionadas no exemplo anterior. É importante observar que AWS Organizations permite a marcação de contas e unidades organizacionais (OUs), no entanto, essas tags não serão aplicáveis à alocação de custos e relatórios de faturamento (ou seja, você não pode agrupar ou filtrar seus custos AWS Cost Explorer por OU). AWS Cost Categories devem ser usadas para essa finalidade.
- Baseado em tags: esse modelo exige mais esforço em comparação com os dois anteriores e fornecerá alta precisão para showbacks e estornos, dependendo dos requisitos e da meta final. Embora seja altamente recomendável que você adote as práticas descritas no whitepaper Organizando seu AWS ambiente usando várias contas, realisticamente, os clientes geralmente se deparam com estruturas de contas mistas e complexas que demoram para serem migradas. A implementação de uma estratégia de marcação rigorosa e eficaz é a chave nesse cenário, seguida pela ativação de tags relevantes para alocação de custos no console do Billing and Cost Management (em, as tags podem ser ativadas para alocação de custos somente AWS Organizations na conta do Management Payer). Depois que as tags são ativadas para alocação de custos, as ferramentas de visibilidade e alocação de custos mencionadas nos métodos anteriores podem ser usadas para showbacks e estornos. Observe que as tags de alocação de custos não são retrospectivas e só aparecerão nos relatórios de faturamento e nas ferramentas de controle de custos depois de serem ativadas para alocação de custos.

Resumindo, se você precisar controlar os custos por unidade de negócios, você pode usar AWS Cost Categories para agrupar contas vinculadas dentro AWS da Organização adequadamente e visualizar esse agrupamento nos relatórios de faturamento. Ao criar contas separadas para

ambientes de produção e de não produção, você também pode filtrar os custos relacionados aos ambientes em ferramentas como AWS Cost Explorer, por exemplo, ou monitorar esses custos usando o AWS Budgets. Por fim, se seu caso de uso exigir um controle de custos mais detalhados, por exemplo, por workloads ou aplicações individuais, você poderá marcar recursos nessas contas adequadamente, ativar essas chaves de tag para alocação de custos na conta de gerenciamento e filtrar esse custo por chaves de tag nas ferramentas de relatórios de faturamento.

Analisar e aprimorar

Comece identificando os tipos de custos que são importantes para as partes interessadas internas (por exemplo, gasto diário, custo por conta, custo por X, custos amortizados). Ao fazer isso, você pode mitigar os riscos orçamentários associados a gastos inesperados ou anômalos mais rapidamente do que esperar pela fatura finalizada. AWS As tags fornecem a atribuição que permite esses cenários de geração de relatórios. Os insights obtidos com os relatórios podem informar suas ações para mitigar o impacto de gastos anômalos e inesperados nos orçamentos financeiros. Quando há um aumento inesperado nos custos, é importante avaliar se houve um aumento inesperado no valor entregue para que você possa determinar se e qual ação é necessária.

Ao especificar uma interface de rede, tenha em mente as considerações e limitações a seguir:

- AWS Organizations: a alocação de custos em várias contas pode ser realizada por conta, grupos de contas ou grupo de tags criadas para recursos nessas contas. As tags criadas para recursos residentes em contas individuais em AWS Organizations podem ser usadas para alocação de custos somente na conta de gerenciamento.
- AWS Conta - A alocação de custos dentro de uma Conta da AWS pode ser realizada por dimensões adicionais, como serviços ou regiões. É possível marcar ainda mais recursos em uma conta e trabalhar com os grupos dessas tags de recursos.
- Tags de alocação de custos: tanto as tags criadas pelo usuário quanto as geradas pela AWS podem ser ativadas para alocação de custos, se necessário. Ativar tags para alocação de custos no console de faturamento (da conta de gerenciamento em AWS Organizations) ajuda com reembolsos e estornos.
- Categorias de AWS custo - As categorias de custos permitem agrupar contas e agrupar tags (“meta-tagging”) dentro de uma AWS organização, o que fornece ainda mais a capacidade de analisar os custos relacionados a essas categorias por meio de ferramentas como AWS Cost Explorer AWS Orçamentos e Relatório de Custos e Uso. AWS

Realizar showback e estorno para unidades de negócios, equipes ou organizações dentro da empresa

Atribua custos usando seu processo de alocação de custos apoiado por sua estrutura de custos e tags de alocação de custos. As tags podem ser usadas para oferecer showback às equipes que não são diretamente responsáveis pelo pagamento dos custos, mas são responsáveis por terem incorrido nesses custos. Essa abordagem fornece consciência de sua contribuição para os gastos e como esses custos são incorridos. Realize o estorno às equipes diretamente responsáveis pelos custos para recuperar as despesas dos recursos que consumiram e para informá-las sobre esses custos e sobre como foram incorridos.

Eficiência ou valor de medição e circulação KPIs

Concorde com um conjunto de métricas de custo unitário ou KPI para medir o impacto de seus investimentos em gerenciamento financeiro na nuvem. Este exercício cria uma linguagem comum entre as partes interessadas em tecnologia e negócios e conta uma história baseada na eficiência, em vez de uma história focada exclusivamente em gastos absolutos e agregados. Para obter informações adicionais, consulte este blog que fala sobre como as métricas unitárias podem ajudar a criar alinhamento entre as funções de negócios.

Alocar gastos não alocáveis

Dependendo das práticas contábeis da organização, diferentes tipos de cobrança podem exigir tratamento diferente. Identifique os recursos ou categorias de custo que não podem ser marcados. Dependendo dos serviços usados e daqueles planejados para serem usados, concorde com os mecanismos de como tratar e medir esses gastos não alocáveis. Por exemplo, verifique a lista de recursos que são compatíveis com o Grupos de recursos da AWS e o Tag Editor no Guia do usuário do Grupos de recursos da AWS e das tags.

Um exemplo comum de categoria de custo que não pode ser marcada são algumas taxas para descontos baseados em compromissos, como instâncias reservadas (IR) e Savings Plans (SP). Embora as taxas de assinatura e as taxas de SP e IR não utilizadas não possam ser marcadas antes de aparecerem nas ferramentas de relatórios de faturamento, é possível rastrear como os descontos de IR e SP se aplicam a contas, recursos e suas tags no AWS Organizations após o fato. Por exemplo, é AWS Cost Explorer possível analisar o custo amortizado, agrupar esses gastos pelas chaves de tag relevantes e aplicar filtros relevantes ao seu caso de uso. No Relatório de Custos e Uso (CUR) da AWS , você pode filtrar as linhas que correspondem ao uso coberto pelos descontos de IR e SP (leia mais na seção de casos de uso da documentação do CUR) e selecionar as colunas

que são relevantes somente para você. Cada chave de tag ativada para alocação de custos será apresentada em sua própria coluna separada no final do relatório CUR, da mesma forma que é apresentada em outros relatórios de faturamento antigos, como o relatório mensal de alocação de custos. Para referência adicional, consulte AWS Well-Architected Labs para ver exemplos de como obter insights de custo e uso dos dados do CUR.

Relatórios

Além das AWS ferramentas disponíveis para ajudar com reembolsos e estornos, há uma variedade de outras soluções AWS criadas e de terceiros que podem ajudar a monitorar o custo dos recursos etiquetados e medir a eficácia da estratégia de marcação. Dependendo dos requisitos e do objetivo final da organização, pode-se investir tempo e recursos na criação de soluções personalizadas ou na compra de ferramentas fornecidas por um dos parceiros com competência em ferramentas de gerenciamento da Nuvem AWS. Se você decidir criar sua própria ferramenta de alocação de custos de fonte fidedigna com parâmetros controlados relevantes para a empresa, o Relatório de AWS Custo e Uso (CUR) fornece os dados mais detalhados de custo e uso e permite a criação de painéis de otimização personalizados, permitindo filtrar e agrupar por contas, serviços, categorias de custo, etiquetas de alocação de custos e várias outras dimensões. Entre as soluções baseadas em CUR desenvolvidas pela AWS that podem ser usadas como uma dessas ferramentas, confira o Cloud Intelligence Dashboards no site da Well-Architected AWS Labs.

Tags para operações e suporte

Um AWS ambiente terá várias contas, recursos e cargas de trabalho com diferentes requisitos operacionais. As tags podem ser usadas para fornecer contexto e orientação para apoiar as equipes de operações a fim de aprimorar o gerenciamento de seus serviços. As tags também podem ser usadas para fornecer transparência na governança operacional dos recursos gerenciados.

Alguns dos principais fatores que impulsionam a definição consistente de tags operacionais são:

- Para filtrar recursos durante atividades de infraestrutura automatizada. Por exemplo, ao implantar, atualizar ou excluir recursos. Outra é a escalabilidade de recursos para otimização de custos e reduções de uso fora do horário de expediente. Consulte a solução AWS Instance Scheduler para obter um exemplo de trabalho.
- Identificação de recursos isolados ou obsoletos. Os recursos que excederam sua vida útil definida ou foram sinalizados para isolamento por mecanismos internos devem ser marcados adequadamente para auxiliar o pessoal de suporte em sua investigação. Os recursos obsoletos devem ser marcados antes do isolamento, arquivamento e exclusão.

- Requisitos de suporte para um grupo de recursos. Os recursos geralmente têm requisitos de suporte diferentes; por exemplo, esses requisitos podem ser negociados entre equipes ou definidos como parte da criticidade de uma aplicação. Mais orientações sobre modelos operacionais podem ser encontradas no Pilar Excelência operacional.
- Melhore o processo de gerenciamento de incidentes. Ao marcar recursos com tags que oferecem maior transparência no processo de gerenciamento de incidentes, as equipes de suporte e os engenheiros, bem como as equipes de gerenciamento de incidentes graves (MIM), podem gerenciar eventos com maior eficiência.
- Backups. As tags também podem ser usadas para identificar a frequência com que seus recursos precisam ser copiados e para onde as cópias de backup precisam ir ou para onde restaurá-las. Orientação prescritiva para abordagens de backup e recuperação sobre. AWS
- Aplicação de patches. A correção de instâncias mutáveis em execução AWS é crucial tanto em sua estratégia abrangente de patches quanto na correção de vulnerabilidades de dia zero. Orientações mais detalhadas sobre a estratégia mais ampla de aplicação de patches podem ser encontradas na orientação prescritiva. A correção de vulnerabilidades de dia zero é discutida neste blog.
- Observabilidade operacional. Ter uma estratégia de KPI operacional traduzida em tags de recursos ajudará as equipes de operações a monitorar melhor se as metas estão sendo cumpridas para aprimorar os requisitos de negócios. Desenvolver uma estratégia de KPI é um tópico separado, mas tende a se concentrar em uma empresa que opera em um estado estável ou onde medir o impacto e os resultados da mudança. Os KPI Dashboards (AWS Well-Architected labs) e o Operations KPI Workshop (um serviço proativo do AWS Enterprise Support) abordam a medição do desempenho em um estado estável. O artigo do blog de estratégia AWS corporativa Measuring the Success of Your Transformation explora a medição de KPI para um programa de transformação, como a modernização da TI ou a migração do local para o. AWS

Automação de infraestrutura

As tags podem ser usadas em uma ampla variedade de atividades de automação ao gerenciar a infraestrutura. O uso do AWS Systems Manager, por exemplo, permitirá que você gerencie automações e runbooks em recursos especificados pelo par de chave-valor definido que você criar. Para nós gerenciados, você pode definir um conjunto de tags para rastrear ou direcionar nós por sistema operacional e ambiente. Em seguida, você pode executar um script de atualização para todos os nós em um grupo ou revisar o status desses nós. Os Recursos do Systems Manager também podem ser marcados para refinar e rastrear ainda mais suas atividades automatizadas.

Automatizar o ciclo de vida inicial e final dos recursos do ambiente pode proporcionar uma redução significativa de custos para qualquer organização. O Instance Scheduler na AWS é um exemplo de solução que pode iniciar e interromper instâncias do Amazon EC2 e do Amazon RDS quando elas não são necessárias. Por exemplo, ambientes de desenvolvedores que utilizam instâncias do Amazon EC2 ou do Amazon RDS que não precisam ser executadas nos finais de semana não estão utilizando o potencial de redução de custos que o encerramento dessas instâncias pode oferecer. Ao analisar as necessidades das equipes e de seus ambientes e marcar adequadamente esses recursos para automatizar seu gerenciamento, você pode utilizar seu orçamento de forma eficaz.

Um exemplo de tag de agendamento usada pelo agendador de instâncias em uma instância do Amazon EC2:

```
{
    "Tags": [
        {
            "Key": "Schedule",
            "ResourceId": "i-1234567890abcdef8",
            "ResourceType": "instance",
            "Value": "mon-9am-fri-5pm"
        }
    ]
}
```

Ciclo de vida da workload

Analise a precisão dos dados operacionais de suporte. Certifique-se de que haja análises periódicas das tags associadas ao ciclo de vida da workload e que as partes interessadas apropriadas estejam envolvidas nessas análises.

Tabela 7: Análise das tags operacionais como parte do ciclo de vida da workload

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Proprietário da conta	`example-inc:account-owner:owner`	O proprietário da conta e seus recursos contidos.	`ops-center` , `dev-ops`, `app-team`
Revisão do proprietário da conta	`example-inc:account-owner:review`	Análise de que os detalhes de propriedade da conta	<review date in the correct format defined

Caso de uso	Chave de tag	Lógica	Valores de exemplo
		estão atualizados e corretos.	in your tagging library>
ID de usuário	`example-inc:data-owner:owner`	O proprietário dos dados das contas que residem nos dados.	`bi-team`, `logistics` , `security`
Analisar o proprietário	`example-inc:data-owner:review`	Revisão dos detalhes de propriedade dos dados que estão atualizados e corretos.	<review date in the correct format defined in your tagging library>

Atribuição de tags às contas suspensas antes de migrar para a UO suspensa

Antes de suspender uma conta e passar para a OU suspensa, conforme detalhado no whitepaper Organizando seu AWS ambiente usando várias contas, as tags devem ser adicionadas à conta para ajudar no rastreamento interno e na auditoria do ciclo de vida de uma conta. Por exemplo, um URL relativo ou uma referência de tíquete no sistema de tíquetes ITSM de uma organização, que mostra a trilha de auditoria de uma aplicação que está sendo suspensa.

Tabela 8: Adição de tags operacionais quando o ciclo de vida da workload entrar em um novo estágio

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Proprietário da conta	`example-inc:account-owner:owner`	O proprietário da conta e seus recursos contidos.	`ops-center` , `dev-ops`, `app-team`
ID de usuário	`example-inc:data-owner:owner`	O proprietário dos dados das contas que residem nos dados.	`bi-team`, `logistics` , `security`

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Data de suspensão	`example-inc:suspension:date`	A data em que a conta foi suspensa	<suspended date in the correct format defined in your tagging library>
Aprovação para suspensão	`example-inc:suspension:approval`	O link para a aprovação da suspensão da conta	`workload/deprecation`

Gerenciamento de incidentes

As tags podem desempenhar um papel vital em todas as fases do gerenciamento de incidentes, desde o registro em log de incidentes, a priorização, a investigação, a comunicação e a resolução até o encerramento.

As tags podem detalhar onde um incidente deve ser registrado em log, a equipe ou equipes que devem ser informadas sobre o incidente e a prioridade de encaminhamento definida. É importante lembrar que as tags não são criptografadas, então considere quais informações você armazena nelas. Além disso, em organizações, equipes e linhas de relatórios, as responsabilidades mudam, então considere armazenar um link para um portal seguro onde essas informações possam ser gerenciadas com mais eficiência. Ao especificar a política, tenha em mente as considerações e limitações. Por exemplo, o ID da aplicação pode ser usado para pesquisar os caminhos de encaminhamento em um portal de gerenciamento de serviços de TI. Certifique-se de que esteja claro em suas definições operacionais que essa tag está sendo usada para várias finalidades.

As tags de requisitos operacionais também podem ser detalhadas para ajudar os gerentes de incidentes e a equipe de operações a refinar ainda mais seus objetivos em resposta a um incidente ou evento.

Links relativos (para o URL base do sistema de conhecimento) para runbooks e manuais podem ser incluídos como tags para ajudar as equipes respondentes a identificar o processo, o procedimento e a documentação correspondentes.

Tabela 9: Uso de tags operacionais para informar o gerenciamento de incidentes

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Gerenciamento de incidentes	`example-inc:incident-management:escalationlog`	O sistema em uso pela equipe de suporte para registrar incidentes	`jira`, `servicenow` , `zendesk`
Gerenciamento de incidentes	`example-inc:incident-management:escalationpath`	Caminho de escalação	`ops-center` , `dev-ops`, `app-team`
Alocação de custos e gerenciamento de incidentes	`example-inc:cost-allocation:CostCenter`	Monitore os custos por centro de custo. Este é um exemplo de uma tag de uso duplo em que o centro de custos está sendo usado como um código de aplicação para registro em log de incidentes	`123-*`
Programação de backup	`example-inc:backup:schedule`	Programação de backup do recurso	`Daily`
Manual/gerenciamento de incidentes	`example-inc:incident-management:playbook`	Manual documentado	`webapp/incident/playbook`

Aplicação de patches

As organizações podem automatizar sua estratégia de aplicação de patches para ambientes de computação mutáveis e manter as instâncias mutáveis alinhadas com a lista de referência de patches definida desse ambiente de aplicação usando o Gerenciador de Patches do AWS

Systems Manager e o AWS Lambda. Uma estratégia de marcação para instâncias mutáveis nesses ambientes pode ser gerenciada atribuindo essas instâncias a grupos de patches e janelas de manutenção. Veja os exemplos a seguir para uma divisão Dev → Test → Prod. AWS uma orientação prescritiva está disponível para o gerenciamento de patches de instâncias mutáveis.

Tabela 10: As tags operacionais podem ser específicas do ambiente

Desenvolvimento	Preparação	Produção
{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab111", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#1 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab222", "ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab333", "ResourceType": "instance", "Value": "WEBAPP-DEV-AL2" }]	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab444", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#2 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab555", "ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab666", "ResourceType": "instance", "Value": "WEBAPP-TEST-AL2" }]	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab777", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#3 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab888", "ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab999", "ResourceType": "instance", "Value": "WEBAPP-PROD-AL2" }]

Desenvolvimento	Preparação	Produção
}	}	}

As vulnerabilidades de dia zero também podem ser gerenciadas com tags definidas para complementar sua estratégia de patches. Consulte Evite vulnerabilidades de dia zero com patches de segurança no mesmo dia usando o Systems AWS Manager para obter orientação detalhada.

Observabilidade operacional.

A observabilidade é necessária para obter insights acionáveis sobre o desempenho de seus ambientes e ajudá-lo a detectar e investigar problemas. Ele também tem uma finalidade secundária que permite definir e medir os principais indicadores de desempenho (KPIs) e objetivos de nível de serviço (SLOs), como tempo de atividade. Para a maioria das organizações, operações importantes KPIs são o tempo médio de detecção (MTTD) e o tempo médio de recuperação (MTTR) de um incidente.

Em toda a observabilidade, o contexto é importante, porque os dados são coletados e, em seguida, as tags associadas são coletadas. Independentemente do serviço, aplicação ou nível de aplicação em que você está se concentrando, você pode filtrar e analisar esse conjunto de dados específico. As tags podem ser usadas para automatizar a integração de CloudWatch alarmes, para que as equipes certas possam ser alertadas quando determinados limites métricos forem violados. Por exemplo, uma chave de tag `example-inc:ops:alarm-tag` e o valor nela podem indicar a criação do CloudWatch alarme. Uma solução que demonstra isso está descrita em Use tags para criar e manter CloudWatch alarmes da Amazon para instâncias do Amazon EC2.

Ter muitos alarmes configurados pode criar facilmente uma tempestade de alertas, quando um grande número de alarmes ou notificações sobrecarrega rapidamente os operadores e reduz sua eficácia geral, enquanto os operadores fazem a triagem e priorizam manualmente os alarmes individuais. Um contexto adicional para os alarmes pode ser fornecido na forma de tags, o que significa que as regras podem ser definidas na Amazon EventBridge para ajudar a garantir que o foco seja dado ao problema inicial, e não às dependências posteriores.

O papel das operações paralelas geralmente DevOps é negligenciado, mas para muitas organizações, as equipes de operações centrais ainda fornecem uma primeira resposta crítica fora do horário comercial normal. (Mais detalhes sobre esse modelo podem ser encontrados no whitepaper de Excelência operacional.) Diferentemente da DevOps equipe responsável pela carga de trabalho, ela normalmente não tem a mesma profundidade de conhecimento. Portanto, o

contexto que as tags fornecem nos painéis e alertas pode direcioná-las para o runbook correto para o problema ou iniciar um runbook automatizado (consulte a postagem do blog Automatizando os alarmes da Amazon com). CloudWatch AWS Systems Manager

Tags para segurança de dados, gerenciamento de riscos e controle de acesso

As organizações têm necessidades e obrigações variadas a cumprir em relação ao tratamento adequado do armazenamento e processamento de dados. A classificação de dados é um precursor importante para vários casos de uso, como controle de acesso, retenção de dados, análise de dados e conformidade.

Segurança de dados e gerenciamento de riscos

Em um AWS ambiente, você provavelmente terá contas com diferentes requisitos de conformidade e segurança. Por exemplo, você pode ter um sandbox para desenvolvedores e uma conta hospedando o ambiente de produção para uma workload altamente regulamentada, como processamento de pagamentos. Ao isolá-los em contas diferentes, é possível aplicar controles de segurança distintos, restringir o acesso a dados confidenciais e reduzir o escopo da auditoria para workloads regulamentadas.

A adoção de um padrão único para todas workloads pode gerar desafios. Embora muitos controles se apliquem igualmente em um ambiente, alguns são excessivos ou irrelevantes para contas que não precisam atender a estruturas regulatórias específicas e contas em que nenhum dado pessoal identificável estará presente (por exemplo, um sandbox para desenvolvedores ou contas de desenvolvimento de workload). Isso normalmente leva a descobertas de segurança falsas positivas que devem ser triadas e encerradas sem nenhuma ação, o que retira o esforço das descobertas que devem ser investigadas.

Tabela 11: Exemplos de tags de segurança de dados e gerenciamento de riscos

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Gerenciamento de incidentes	`example-inc:incident-management:escalationlog`	O sistema em uso pela equipe de suporte para registrar incidentes	`jira`, `servicenow` , `zendesk`

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Gerenciamento de incidentes	`example-inc:incident-management:escalationpath`	Caminho de escalação	`ops-center` , `dev-ops`, `app-team`
Classificação de dados	`example-inc:data:classification`	Classifique os dados para fins de conformidade e governança	`Public`, `Private`, `Confidential` , `Restricted`
Compliance	`example-inc:compliance:framework`	Identifica a estrutura de conformidade à qual a workload está sujeita	`PCI-DSS`, `HIPAA`

O gerenciamento manual de diferentes controles em um AWS ambiente é demorado e propenso a erros. A próxima etapa é automatizar a implantação dos controles de segurança apropriados e configurar a inspeção dos recursos com base na classificação dessa conta. Ao aplicar tags às contas e aos recursos dentro delas, a implantação de controles pode ser automatizada e configurada adequadamente para a workload.

Exemplo:

Uma workload inclui um bucket do Amazon S3 com a tag `example-inc:data:classification` e o valor `Private`. A automação das ferramentas de segurança implanta a AWS Config regras`3-bucket-public-read-prohibited`, que verifica as configurações de bloqueio de acesso público do bucket Amazon S3, a política do bucket e a lista de controle de acesso (ACL) do bucket, confirmando que a configuração do bucket é apropriada para sua classificação de dados. Para garantir que o conteúdo do bucket seja consistente com a classificação, o Amazon Macie pode ser configurado para verificar as informações de identificação pessoal (PII). O blog Using Amazon Macie to Validate S3 Bucket Data Classification explora esse padrão com mais profundidade.

Certos ambientes regulatórios, como seguros e assistência médica, podem estar sujeitos a políticas obrigatórias de retenção de dados. A retenção de dados usando tags, combinada com as políticas de ciclo de vida do Amazon S3, pode ser uma forma eficaz e simples de definir o escopo das transições de objetos para um nível de armazenamento diferente. As regras de ciclo de vida do Amazon S3 também podem ser usadas para expirar objetos para exclusão de dados após o término do período

de retenção obrigatório. Consulte Simplify your data lifecycle by using object tags with Amazon S3 Lifecycle para obter um guia detalhado desse processo.

Além disso, ao fazer a triagem ou abordar as descobertas de segurança, as tags podem fornecer ao investigador um contexto importante que ajuda a qualificar o risco e ajuda a engajar as equipes apropriadas para investigar ou mitigar a descoberta.

Tags para gerenciamento de identidade e controle de acesso

Ao gerenciar o controle de acesso em um AWS ambiente com Centro de Identidade do AWS IAM, as tags podem habilitar vários padrões de escalabilidade. Existem vários padrões de delegação que podem ser aplicados, alguns são baseados na marcação. Nós os abordaremos individualmente e forneceremos links para leituras adicionais sobre cada um.

ABAC recursos individuais

Os perfis do IAM e os usuários do Centro de Identidade do IAM comportam controle de acesso por atributo (ABAC), que permite definir o acesso a operações e recursos com base em tags. O ABAC ajuda a reduzir a necessidade de atualizar as políticas de permissão e ajuda você a basear o acesso nos atributos dos funcionários do seu diretório corporativo. Se você já estiver usando uma estratégia de várias contas, o ABAC pode ser usado além do controle de acesso baseado em funções (RBAC) para fornecer a várias equipes que operam na mesma conta acesso granular a diferentes recursos. Por exemplo, perfis do IAM ou usuários do Centro de Identidade do IAM podem incluir condições para limitar o acesso a instâncias específicas do Amazon EC2 que, de outra forma, precisariam ser listadas explicitamente em cada política para acessá-las.

Como um modelo de autorização ABAC depende de tags para acesso às operações e aos recursos, é importante fornecer grades de proteção para evitar o acesso não intencional. SCPs pode ser usado para proteger as tags em toda a sua organização, permitindo que as tags sejam modificadas somente sob determinadas condições. Os blogs Securing resource tags used for authorization using a service control policy in AWS Organizations e Permissions boundaries for IAM entities fornecem informações sobre como implementar isso.

No caso que instâncias de longa duração do Amazon EC2 estão sendo usadas para atender a práticas operacionais mais tradicionais, essa abordagem pode ser utilizada. O blog Configure IAM Identity Center ABAC for Amazon EC2 instances and Systems Manager Session Manager discute essa forma de controle de acesso baseado em atributos com mais detalhes. Conforme mencionado anteriormente, nem todos os tipos de recursos oferecem suporte à marcação e, dos que oferecem,

nem todos oferecem suporte à fiscalização usando políticas de tags. Portanto, é uma boa ideia avaliar isso antes de começar a implementar essa estratégia em uma Conta da AWS.

Para saber mais sobre os serviços que oferecem suporte ao ABAC, consulte serviços AWS que funcionam com o IAM.

Conclusão

AWS os recursos podem ser marcados para diversas finalidades, desde a implementação de uma estratégia de alocação de custos até o suporte à automação ou a autorização do acesso aos AWS recursos. A implementação de uma estratégia de marcação pode ser um desafio para algumas organizações, devido ao número de grupos de partes interessadas envolvidos e a considerações como fornecimento de dados e governança de tags.

Neste whitepaper, descrevemos recomendações sobre como projetar e implementar uma estratégia de marcação em uma organização com base em práticas operacionais, casos de uso definidos, partes interessadas envolvidas no processo e ferramentas e serviços fornecidos pela AWS. Quando se trata de uma estratégia de marcação, é um processo de iteração e melhoria, em que você começa aos poucos a partir de sua prioridade imediata, identifica casos de uso relevantes em toda a organização e, em seguida, implementa e expande o esquema de marcação conforme necessário, enquanto mede e melhora continuamente a eficácia. Destacamos que um conjunto bem definido de tags em sua organização permitirá que você relacione o AWS uso e o consumo às equipes responsáveis pelos recursos e pela finalidade comercial para os quais eles existem, a fim de se alinhar à estratégia e ao valor organizacionais.

Colaboradores

Os colaboradores deste documento incluem:

- Chris Pates, gerente técnico sênior de contas técnicas, Amazon Web Services
- Vijay Shekhar Rao, líder de suporte corporativo, Amazon Web Services
- Nataliya Godunok, gerente técnica sênior de contas técnicas, Amazon Web Services
- Yogish Kutkunje Pai, arquiteto sênior de soluções, Amazon Internet Services Private Limited
- Jamie Ibbs, gerente técnico sênior de contas técnicas, Amazon Web Services

Outras fontes de leitura

Para obter mais informações, consulte os seguintes recursos:

- AWS re:Invent 2020: trabalhando de trás para frente: a abordagem da Amazon à inovação
- AWS Orientação prescritiva: correção automatizada para instâncias mutáveis na nuvem híbrida usando o Systems Manager AWS
- AWS Centro de Arquitetura

AWS Well-Architected

- AWS Well-Architected Framework
- Pilar de excelência operacional - AWS Well-Architected Framework
- Plano de recuperação de desastres (DR) - pilar de confiabilidade AWS Well-Architected
- Pilar de otimização de custos - AWS Well-Architected Framework
- AWS Well-Architected Labs: AWS habilite tags de alocação de custos geradas
- AWS Well-Architected Labs: políticas de tags
- AWS Well-Architected Labs AWS : Biblioteca de consultas CUR

AWS blogs

- AWS Health Aware — Personalize AWS Health alertas para AWS contas pessoais e organizacionais
- Como marcar automaticamente EC2 os recursos da Amazon em resposta a eventos da API
- AWS Etiqueta de alocação de custos gerada versus definida pelo usuário
- Etiquetagem e relatórios de custos com AWS Organizations
- Corrigindo suas EC2 instâncias do Windows usando o AWS Systems Manager Patch Manager
- Evite vulnerabilidades de dia zero com patches de segurança no mesmo dia usando AWS Systems Manager

AWS documentação

- Usando tags de alocação de custos - Gerenciamento de Faturamento e Custos da AWS

- O que são relatórios de AWS custo e uso
- Grupos de recursos da AWS API Reference
- Como posso usar tags de política do IAM para restringir como uma EC2 instância ou volume do EBS pode ser criado?
- Mutable vs immutable update models

Outros

- Bryar, C. e Carr, B. (2021). Working Backwards: Insights, Stories, and Secrets from Inside Amazon. Londres, Macmillan.
- AWS CloudFormation Guarda (GitHub)

Revisões do documento

Para ser notificado sobre atualizações desse whitepaper, inscreva-se no feed RSS.

Alteração	Descrição	Data
Atualização secundária	Orientação esclarecida para recomendar não usar chaves que diferem apenas na caixa.	10 de junho de 2025
Atualização secundária	CloudEndure Referênci as alteradas para AWS Transform MGN.	8 de maio de 2025
Atualização secundária	Atualizações no gerenciam ento de identidade	30 de março de 2023
Revisão secundária	Referência atualizada no ABAC para recursos individua is.	24 de fevereiro de 2023
Revisão secundária	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para saber mais, consulte Práticas recomendadas de segurança no IAM.	6 de fevereiro de 2023
Revisões importantes	Foi adicionada uma referênci a mais específica para os tipos de recursos suportados pela AWS Config regra `required_tags` .	18 de janeiro de 2023
Revisões importantes	Atualizado para incluir as práticas e os recursos de serviço mais recentes,	29 de setembro de 2022

	especialmente na área de identidade.	
Atualização secundária	Formatação de tabela fixa na versão PDF.	25 de abril de 2022
Revisões importantes	Estrutura de documentos atualizada e seções expandidas de estratégia de marcação e casos de uso. Foram adicionadas mais orientações prescritivas com base nas ferramentas, técnicas e recursos disponíveis mais recentes.	22 de abril de 2022
Publicação inicial	O whitepaper foi publicado pela primeira vez.	1º. de dezembro de 2018

> **Note**
>
> Para assinar as atualizações de RSS, você deve ter um plug-in RSS habilitado para o navegador que você está usando.

Avisos

Os clientes são responsáveis por fazer a própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas atuais de AWS produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “como estão” sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e obrigações de AWS seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum contrato entre AWS e seus clientes.

© 2022 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

AWS Glossário

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

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.