Whitepapers da AWS

Práticas recomendadas para políticas

Práticas recomendadas para políticas: Whitepapers da AWS

Table of Contents

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 atribuir metadados a muitos de seus recursos AWS 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 e o uso de custos, bem como o gerenciamento de seu ambiente AWS.

Este artigo se baseia nas práticas e orientações fornecidas no whitepaper Organização do seu AWS ambiente usando várias contas. Recomenda-se que você leia aquele whitepaper antes deste. A AWS recomenda que você estabeleça sua base na nuvem de maneira holística. Para obter informações adicionais, consulte Estabelecimento de sua base na nuvem na AWS.

Sua arquitetura está bem planejada?

O AWSWell-Architected Framework ajuda você a entender os prós e os contras das decisões tomadas ao criar sistemas na nuvem. Os seis pilares do Framework permitem que você aprenda as melhores práticas arquitetônicas para projetar e operar sistemas confiáveis, seguros, eficientes, economicamente viáveis e sustentáveis. Usando o AWS Well-Architected Tool, disponível gratuitamente no AWS Management Console, você pode analisar seus workloads em relação a essas melhores práticas respondendo a um conjunto de perguntas para cada pilar.

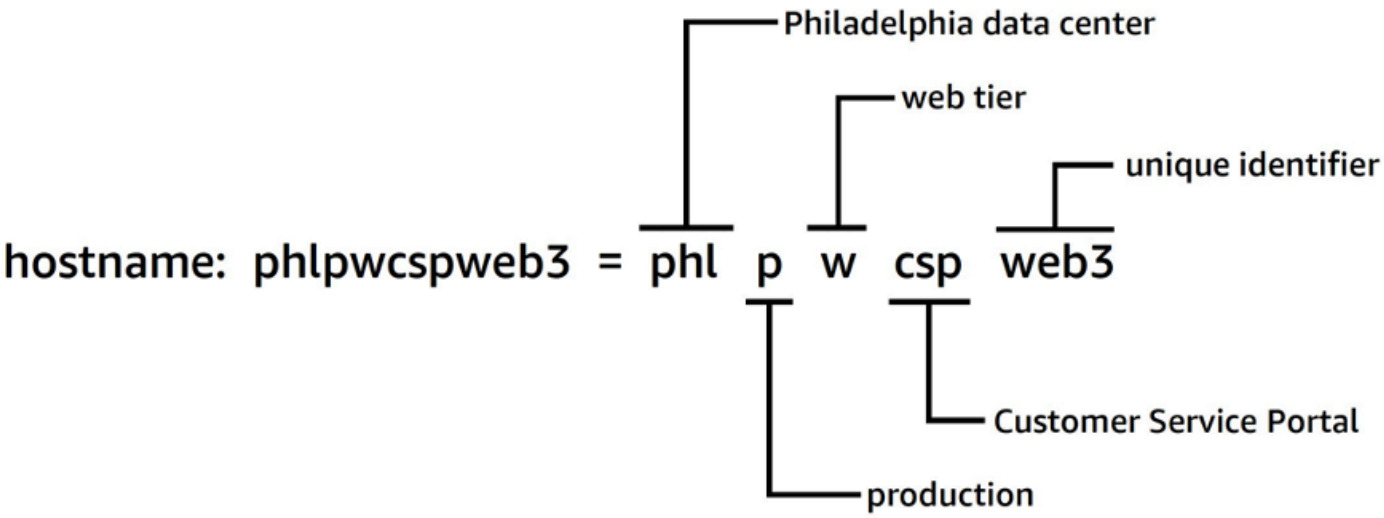
Para obter orientações especializadas e melhores práticas adicionais para a arquitetura de sua nuvem (implantações de arquitetura de referência, diagramas e whitepapers), consulte o Centro de arquitetura da AWS.

Introdução

A AWS facilita a implantação de seus workloads na AWS por meio da criação de recursos, como instâncias do Amazon EC2, volumes do Amazon EBS, grupos de segurança e AWS Lambda funções. Você também pode escalar e aumentar a frota de recursos AWS que hospeda seus aplicativos, armazena seus dados e expande sua infraestrutura AWS ao longo do tempo. À medida que seu uso da AWS 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 locais, 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, a AWS lançou as 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 valores-chave 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 Serviços compatíveis com a API Resource Groups Tagging). Outros serviços podem oferecer suporte a tags por meio de suas próprias 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 AWS Management Console são conhecidas como tags definidas pelo usuário. Vários serviços AWS como o AWS CloudFormation, 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 recurso AWS. Para obter mais informações, consulte Limites e requisitos de nomeação de tags no guia de referência geral da AWS. As tags geradas pela AWS não contam para esses 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 geradas pela AWS

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

As tags geradas pela AWS formam um namespace. Por exemplo, em um modelo AWS CloudFormation, você define um conjunto de recursos a serem implantados juntos em um `stack`, em que `stack-name` é 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: aws, a organização, cloudformation, o serviço, e stack-name, o parâmetro.

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 Estabelecendo sua base na nuvem 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

Organização	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 que trabalham com um provedor de serviços gerenciados, editor de jogos ou empresa de capital de risco, em que contas de diferentes organizações fazem parte de uma organização AWS 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

Organização	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 etiquetas 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 Marcação de recursos da AWS 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.

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 da estratégia, iteração e 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, Responsável, 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.

Definindo 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:

- As finanças e a linha de negócios precisam entender o valor do investimento mapeando-o aos custos para priorizar as ações que precisam ser tomadas 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, confidenciais ou confidenciais), se uma carga de trabalho 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 aplicativo 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 carga de trabalho, os estágios implementados de seus produtos suportados 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. O InfoSec normalmente define a implementação dos controles, e o SecOps geralmente 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 aplicativos 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 etiquetas obrigatórias e podem recomendar o escopo das etiquetas 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.

Definindo e publicando um esquema de marcação

Use uma abordagem consistente para marcar seus recursos AWS, 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 prefixo de valor/ suv/x)	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`	Y	Tudo	Tudo	Obrigatório
Alocação de custos	`example-inc:cost-allocation: BusinessUnitId`	Monitore os custos por unidade de negócios	`Architecture` , `DevOps`, `Finance`	Y	Tudo	Tudo	Obrigatório
Alocação de custos	`example-inc:cost-allocation: CostCenter`	Monitore os custos por centro de custo	`123-*`	Y	Tudo	Tudo	Obrigatório
Alocação de custos	`example-inc:cost-allocation :Owner`	Qual detentor do orçamento é responsável por essa carga de trabalho	`Marketing` , `RetailSupport`	Y	Tudo	Tudo	Obrigatório
Controle de acesso	`example-inc:access-control:`	Identifique o subcomponente/camada	`DB_Layer`, `Web_Layer` , `App_Layer`	N	Tudo	Tudo	Optional

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

Caso de uso	Chave de tag	Lógica	Valores permitidos (listados ou prefixo de valor/ suv/x)	Usado para alocação de custos	Tipos de recursos	Escopo	Obrigatório
DevOps	`example-inc:operations: Owner`	Qual equipe/ esquadrão é responsável pela criação e manutenção do recurso	`Squad01`	N	Tudo	Tudo	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	Tudo	Obrigatório
Conformidade	`example-inc:compliance: framework`	Identifica a estrutura de conformidade à qual a carga de trabalho está sujeita	`PCI-DSS`, `HIPAA`	N	Tudo	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 marcação

As políticas no AWS Organizations permitem que você aplique tipos adicionais de governança às 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.

Exemplo em c-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-*"
        ]
      }
    }
  }
}
```

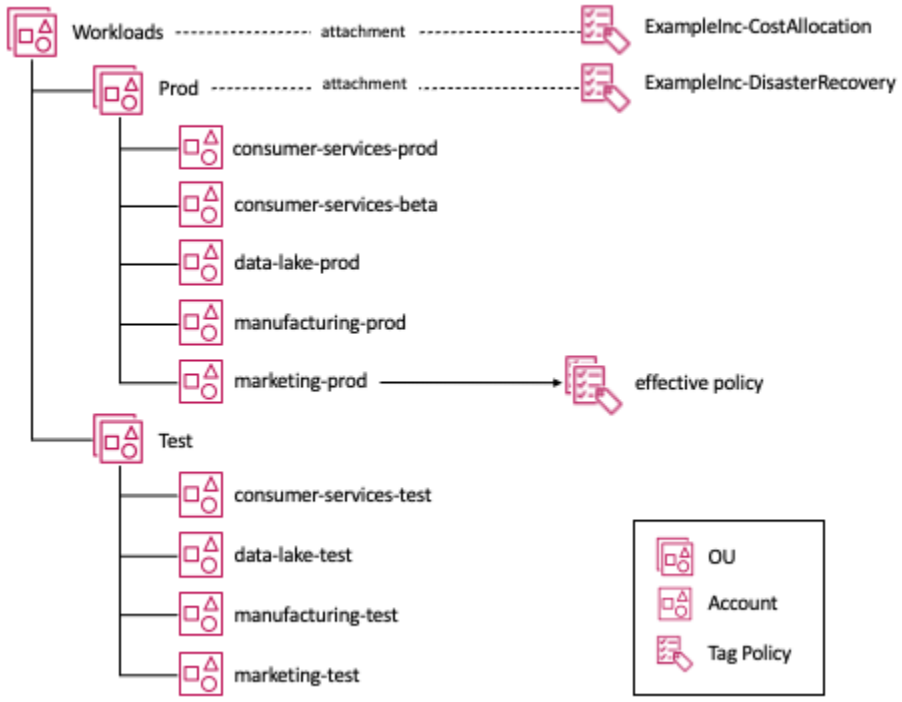
Exemplo em c-disasterrecovery.json

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 Organizando seu ambiente usando várias contas 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 Resource Groups & Tag Editor:Tag policies no console. Se você usa infraestrutura como código (IaC) ou scripts para gerenciar seus recursos, você pode usar a chamada de `AWS::Organizations::DescribeEffectivePolicy`API.

Implementando e aplicando a marcação

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

Recursos gerenciados manualmente

Normalmente, são cargas de trabalho que se enquadram nos estágios de fundação ou migração da adoção. Em geral, são cargas de trabalho simples e amplamente estáticas que foram criadas usando procedimentos tradicionais escritos ou migradas como estão usando ferramentas como o CloudEndure de um ambiente local. Ferramentas de migração, como o Migration Hub e o CloudEndure, 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 AWS Management Console) 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 de marcação de recursos da AWS permite que você execute essas funções de forma programática.

À medida que essas cargas de trabalho são modernizadas, tipos de recursos, como grupos de Auto Scaling, são introduzidos. Esses tipos de recursos permitem maior elasticidade e maior resiliência. O grupo de 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 carga de trabalho estão sendo gerenciados manualmente, pode ser útil automatizar a marcação de recursos. Há várias soluções disponíveis. Uma abordagem é usar o Regras do AWS Config, que pode verificar se há `required_tags` e, em seguida, iniciar uma função Lambda para aplicá-los. O Regras do AWS Config é descrito em mais detalhes posteriormente neste whitepaper.

Recursos gerenciados de infraestrutura como código (IaC)

O AWS CloudFormation fornece uma linguagem comum para o provisionamento de todos os recursos de infraestrutura em seu ambiente AWS. Os modelos do CloudFormation são arquivos JSON ou YAML que criam recursos da AWS de forma automatizada. Ao criar recursos AWS usando modelos do CloudFormation, 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 pelo AWS CloudFormation, o serviço aplica automaticamente um conjunto de tags definidas pela AWS aos recursos criados pelo modelo do AWS CloudFormation. 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 pilha AWS CloudFormation. Essas tags AWS definidas são herdadas pelos recursos criados pela pilha. No entanto, para instâncias do Amazon EC2 dentro de um grupo de Auto Scaling, o `AWS::AutoScaling::AutoScalingGroupTagProperty` precisa ser definido 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 Auto Scaling, poderá definir as tags em sua definição. Recomenda-se usar os modelos de inicialização do EC2 com grupos de dimensionamento automático ou com um serviço de contêiner da AWS. 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.

Os ganchos AWS CloudFormation fornecem aos desenvolvedores um meio de manter os principais aspectos de seus aplicativos consistentes com os padrões da organização. Os ganchos 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 serão iniciadas 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 ganchos AWS CloudFormation antes da implantação.

O 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 ganchos AWS CloudFormation e publicar conjuntos de regras do AWS CloudFormation Guard que possam ser usados pela automação.

Recursos gerenciados do pipeline de CI/CD

À medida que a maturidade de uma carga de trabalho aumenta, é provável que sejam adotadas técnicas como a integração contínua e a implantação contínua (CI/CD). 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 fazer essas verificações o mais cedo possível no processo (como mostrado nos hooks do AWS CloudFormation), para que você possa ter certeza de que o modelo do AWS CloudFormation atende às suas políticas antes de sair do computador do desenvolvedor.

O AWS CloudFormationGuard 2.0 fornece os meios para escrever regras preventivas de conformidade para qualquer coisa que você possa definir com o 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 o `AWS::AutoScaling::AutoScalingGroupTagProperty` estivesse sempre sendo usado.

Veja a seguir um exemplo de uma política de endpoints do CloudFormation.

```
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, o Resource 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 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

A seguir, um exemplo de política de tag que relata e/ou aplica 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`**)

O AWS Config é um serviço que permite avaliar, auditar e analisar as configurações dos seus recursos do AWS (consulte Tipos de recursos suportados pelo 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 Tipos de recursos suportados por 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 modelo AWS CloudFormation descreve uma regra AWS Config 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 regra AWS Config pode ser aprimorada para adicionar automaticamente a chave de tag ausente aos recursos usando uma correção automatizada por meio de uma função AWS Lambda. Embora isso funcione bem para cargas de trabalho 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 pode ser usada para gerenciar permissões na sua organização. As SCPs oferecem controle central sobre as permissões máximas disponíveis para todas as contas da sua organização ou unidade organizacional (OU). 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:

```
{
  "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 eventos do CloudTrail em sua conta pode ajudar os desenvolvedores na tarefa de depuração quando seus recursos não estão em conformidade.

Medindo a eficácia da marcação e promovendo 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 AWS Cost Explorer ou Relatório de Custos e Uso 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 adoção AWS. O aumento da responsabilidade pela segurança e pelo custo de desenvolvimento e operação de seus aplicativos

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

Etiquetas 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 cargas de trabalho 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 etiquetados de forma consistente, por exemplo, para recursos do tamanho certo, escalonados automaticamente ou programados.

Entender como você incorre em custos na AWS permite que você tome decisões financeiras informadas. Saber onde você incorreu em custos no nível de recursos, carga de trabalho, 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. A contratação de uma pessoa com habilidades especializadas em gerenciamento financeiro da AWS que possa treinar as equipes de engenharia e desenvolvimento sobre os conceitos básicos do gerenciamento financeiro da AWS e criar um relacionamento entre finanças e engenharia para promover a cultura de FinOps ajudará a obter resultados mensuráveis para os negócios e incentivará as equipes a criar com o custo em mente. O estabelecimento de boas práticas

financeiras é abordado em profundidade pelo Pilar de 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.

Ferramentas e mecanismos de estorno ajudam a aumentar a conscientização sobre os custos. O estorno ajuda na recuperação de custos e impulsiona a conscientização de custos. O showback trata da apresentação, cálculo e geração de relatórios de cobranças incorridas por uma entidade específica, como unidade de negócios, aplicativo, usuário ou centro de custos. Por exemplo: "a equipe de engenharia de infraestrutura foi responsável por $X de gastos com 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 dólares foram deduzidos do orçamento AWS da equipe de engenharia de infraestrutura". Em ambos os casos, marcar recursos de forma adequada pode ajudar a alocar o custo para uma entidade, com a única diferença sendo se se espera ou não que alguém efetue um pagamento.

A governança financeira da sua organização pode exigir uma contabilidade transparente dos custos incorridos no nível do aplicativo, da unidade de negócios, do centro de custos e da equipe. A execução da atribuição de custos suportada pelas Etiquetas 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 para aqueles que são 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 visão clara das alocações de dinheiro para a TI criando painéis eficazes e análises de custos significativas para a liderança.
- Investimentos informados em TI - acompanhe o ROI com base no projeto, aplicativo ou linha de negócios e capacite as equipes a tomarem melhores decisões de negócios, por exemplo, alocando mais fundos para aplicativos geradores de 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 carga de trabalho, aplicativo ou produto está incorrendo nos gastos? Qual ambiente ou palco?
- Quais áreas de gastos estão crescendo mais rápido?
- Quanto gasto pode ser deduzido de um orçamento de AWS com base em tendências anteriores?
- Qual foi o impacto dos esforços de otimização de custos em cargas de trabalho, aplicativos ou produtos específicos?

A ativação de tags 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 uso da AWS, o que aumenta a transparência e a responsabilidade pelos gastos. Também se concentra em criar um nível adequado de granularidade com relação à visibilidade de custo e uso e influenciar os comportamentos de consumo da nuvem por meio de relatórios de alocação de custos e rastreamento de KPI.

Construindo uma estratégia de alocação de custos

Definindo e implementando um modelo de alocação de custos.

Crie uma estrutura de contas e custos para os recursos que estão sendo implementados na AWS. Estabeleça a relação entre os custos de despesas da AWS, como esses custos foram incorridos e quem ou o que incorreu nesses custos. As estruturas de custo comuns são baseadas em ambientes e entidades AWS Organizations, Contas da AWS em 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 diferentes ou em diferentes níveis de granularidade, como transferir os custos de cargas de trabalho 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. Os três modelos populares de alocação de custos com os quais os clientes da AWS geralmente começam 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 ambiente AWS usando várias contas). Isso fornece uma visibilidade clara dos custos por conta. Para

visibilidade e alocação de custos, você pode usar AWS Cost Explorerrelatórios de custo e uso, bem como Orçamentos AWS 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.

- Unidade de negócios ou baseado 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 devoluções e cobranças retroativas e é adequado para organizações que têm uma estrutura de contas definida (normalmente usando AWS Organizations), com separação entre várias equipes, aplicativos e tipos de carga de trabalho. Isso fornece uma visibilidade clara dos custos entre equipes e aplicativos e, como benefício adicional, reduz o risco de atingir as cotas de AWS serviço em um único momento Conta da AWS. Por exemplo, cada equipe pode ter cinco contas (`prod`, `staging`, `test`, `dev`, `sandbox`) e duas equipes e aplicativos não compartilharão a mesma conta. Com essa estrutura, a AWSCost Categories fornecerá a funcionalidade de agrupar contas ou outras tags (“meta-tagging”) em categorias, que podem ser rastreadas nas ferramentas mencionadas no exemplo anterior. É importante observar que o AWS Organizations permite a marcação de contas e unidades organizacionais (OUs); no entanto, essas marcações não serão aplicáveis à alocação de custos e aos relatórios de faturamento (ou seja, você não pode agrupar ou filtrar seus custos no 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 devoluções e estornos, dependendo dos requisitos e da meta final. Embora seja altamente recomendável que você adote as práticas descritas no whitepaper Organizando seu ambiente AWS 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 só podem ser ativadas para alocação de custos 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 devoluções e estornos. Observe que as etiquetas 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 AWSCost Categories para agrupar contas vinculadas dentro da Organização AWS 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 Orçamentos AWS. Por fim, se seu caso de uso exigir um controle de custos mais granular, por exemplo, por cargas de trabalho ou aplicativos 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 da 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 etiquetas criadas para recursos que residem em contas individuais no AWS Organizations podem ser usadas para alocação de custos somente a partir da conta de gerenciamento.
- Conta AWS - 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. A ativação de tags para alocação de custos no console de faturamento (da conta de gerenciamento no AWS Organizations) ajuda com os showbacks e chargebacks.
- Cost Categories - As categorias de custo da AWS permitem o agrupamento de contas e o agrupamento de tags ("meta-tagging") em uma organização da AWS, o que permite analisar o custo relacionado a essas categorias por meio de ferramentas como AWS Cost Explorer, AWS Budgets e AWS Cost and Usage Report.

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

Atribua custos usando seu processo de alocação de custos suportado por sua estrutura de custos e etiquetas de alocação de custos. As etiquetas podem ser usadas para oferecer um retorno 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.

Medição e circulação de KPIs de eficiência ou valor

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.

Alocação de 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 AWS Resource Groups e o Tag Editor no Guia do usuário do AWS Resource Groups e das tags.

Um exemplo comum de categoria de custo que não pode ser etiquetada são algumas taxas para descontos baseados em compromissos, como Instâncias Reservadas (RI) e Savings Plans (SP). Embora as taxas de assinatura e as taxas de SP e RI não utilizadas não possam ser marcadas antes de aparecerem nas ferramentas de relatórios de faturamento, é possível rastrear como os descontos de RI e SP se aplicam a contas, recursos e suas tags no AWS Organizations após o fato. Por exemplo, no AWS Cost Explorer, é possível examinar o custo amortizado, agrupar esse gasto pelas chaves de tag relevantes e aplicar filtros relevantes para seu caso de uso. No Relatório de Custo e Uso (CUR) AWS, você pode filtrar as linhas que correspondem ao uso coberto pelos descontos de RI 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 o AWSWell-Architected Labs para ver exemplos de como obter insights de custo e uso dos dados do CUR.

Relatórios

Além das ferramentas da AWS disponíveis para ajudar com showbacks e chargebacks, há uma série de outras soluções criadas pela AWS e de terceiros que podem ajudar a monitorar o custo dos recursos marcados 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 de competência em ferramentas de Nuvem AWS gerenciamento. Se você decidir criar sua própria ferramenta de alocação de custos de fonte fidedigna com parâmetros controlados relevantes para o negócio, o Relatório de Custo e Uso (CUR) AWS 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.

Etiquetas para operações e suporte

Um ambiente AWS 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 etiquetados adequadamente para auxiliar o pessoal de suporte em sua investigação. Os recursos obsoletos devem ser marcados antes do isolamento, arquivamento e exclusão.

- Support requisitos 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 um aplicativo. Mais orientações sobre modelos operacionais podem ser encontradas no Pilar de Excelência Operacional.
- Melhore o processo de gerenciamento de incidentes. Ao marcar recursos com etiquetas que oferecem maior transparência no processo de gerenciamento de incidentes, equipes de suporte e engenheiros, bem como equipes de Gerenciamento de Incidentes Graves (MIM), podem gerenciar eventos com mais 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 na AWS.
- Aplicação de patches. A correção de instâncias mutáveis em execução na AWS é crucial tanto para sua estratégia de correção abrangente quanto para a 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 etiquetas 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 (AWSWell-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 a AWS.

Automação de infraestrutura

As tags podem ser usadas em uma ampla variedade de atividades de automação ao gerenciar a infraestrutura. O uso do Systems Manager, por exemplo, permitirá que você gerencie automações e runbooks em recursos especificados pelo par de valores-chave 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 agendador de instâncias ativado 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"
        }
    ]
}
```

Automação do ciclo de vida

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

Tabela 7 - Analise as etiquetas operacionais como parte do ciclo de vida da carga de trabalho

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`

Caso de uso	Chave de tag	Lógica	Valores de exemplo
Revisão do proprietário da conta	`example-inc:account-owner:review`	Análise de que os detalhes de propriedade da conta estão atualizados e corretos.	<review date in the correct format defined 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 OU suspensa

Antes de suspender uma conta e passar para a OU suspensa, conforme detalhado no whitepaper Organizando seu ambiente AWS 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, uma URL relativa ou referência de tíquete no sistema de tíquetes ITSM de uma organização, que mostra a trilha de auditoria de um aplicativo que está sendo suspenso.

Tabela 8 - Adicione tags operacionais quando o ciclo de vida da carga de trabalho 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`

Caso de uso	Chave de tag	Lógica	Valores de exemplo
ID de usuário	`example-inc:data-owner:owner`	O proprietário dos dados das contas que residem nos dados.	`bi-team`, `logistics` , `security`
Data de suspensão	`example-inc:suspension:date`	A data em que a conta foi suspensa	<data suspensa no formato correto definido em sua biblioteca de marcação>
Aprovação para suspensão	`example-inc:suspension:approval`	O link para a aprovação da suspensão da conta	`workload/deprecation`

Gerenciamento de incidentes

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

As tags podem detalhar onde um incidente deve ser registrado, a equipe ou equipes que devem ser informadas sobre o incidente e a prioridade de escalonamento 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 do aplicativo pode ser usado para pesquisar os caminhos de escalonamento 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 etiquetas 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 playbooks podem ser incluídos como tags para ajudar as equipes respondentes a identificar o processo, o procedimento e a documentação correspondentes.

Tabela 9 - Use etiquetas 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 etiqueta de uso duplo em que o centro de custos está sendo usado como um código de aplicativo para registro 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 linha de base de patches definida desse ambiente de aplicativo usando o AWS Systems Manager Patch 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 etiquetas operacionais podem ser específicas do ambiente

Desenvolvimento	Preparação	Produção
{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab1 11", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#1 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab2 22", "ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab3 33",	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab4 44", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#2 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab5 55", "ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab6 66",	{ "Tags": [{ "Key": "Maintenance Window", "ResourceId": "i-012345678ab9ab7 77", "ResourceType": "instance", "Value": "cron(30 23 ? * TUE#3 *)" }, { "Key": "Name", "ResourceId": "i-012345678ab9ab8 88", "ResourceType": "instance", "Value": "WEBAPP" }, { "Key": "Patch Group", "ResourceId": "i-012345678ab9ab9 99",

Desenvolvimento	Preparação	Produção
`"ResourceType": "instance", "Value": "WEBAPP-DEV-AL2" } ] }`	`"ResourceType": "instance", "Value": "WEBAPP-TEST-AL2" } ] }`	`"ResourceType": "instance", "Value": "WEBAPP-PROD-AL2" } ] }`

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 AWS Systems 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 indicadores-chave de desempenho (KPIs) e objetivos de nível de serviço (SLOs), como tempo de atividade. Para a maioria das organizações, os KPIs operacionais importantes 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, aplicativo ou nível de aplicativo 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 aos alarmes do CloudWatch, 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 alarme do CloudWatch. Uma solução que demonstra isso está descrita em Use tags para criar e manter alarmes do Amazon CloudWatch 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 no Amazon EventBridge para ajudar a garantir que o foco seja dado ao problema inicial, e não às dependências posteriores.

O papel das operações junto com o DevOps geralmente é esquecido, 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 equipe de DevOps que é proprietária da 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 alarmes do Amazon CloudWatch com). AWS Systems Manager

Etiquetas 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 ambiente AWS, 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 carga de trabalho 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 cargas de trabalho regulamentadas.

A adoção de um padrão único para todas as cargas de trabalho 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 carga de trabalho). 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`
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`
Conformidade	`example-inc:compliance:framework`	Identifica a estrutura de conformidade à qual a carga de trabalho está sujeita	`PCI-DSS`, `HIPAA`

O gerenciamento manual de diferentes controles em um ambiente AWS 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 carga de trabalho.

Exemplo:

Uma carga de trabalho inclui um bucket do Amazon S3 com a tag `example-inc:data:classification` com o valor `Private`. A automação das ferramentas de segurança implanta a regra AWS Config `s3-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 Simplifique seu ciclo de vida de dados usando tags de objetos com o ciclo de vida do Amazon S3 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 ambiente AWS com AWS IAM Identity Center, 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 para o Amazon ABAC

Automação do KMS com base no ABAC (ABAC), o fornece chaves de condição que controlam o acesso a uma chave do KMS. 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, usuários do IAM Identity Center ou funções 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. Os SCPs podem ser usados para proteger as tags em sua organização, permitindo que as tags sejam modificadas somente sob determinadas condições. Por exemplo, é possível definir um conjunto de tags que controlam o acesso a uma política completa com uma análise detalhada do KMS AWS Organizations

Onde instâncias de longa duração do Amazon EC2 estão sendo usadas para apoiar práticas operacionais mais tradicionais, então 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

Os recursos da AWS podem ser marcados para diversas finalidades, desde a implementação de uma estratégia de alocação de custos até a automação de suporte ou a autorização de acesso aos recursos do AWS. 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. Ressaltamos que um conjunto bem definido de tags em sua organização permitirá que você relacione o uso e o consumo da AWS às equipes responsáveis pelos recursos e pela finalidade comercial para os quais eles existem, a fim de alinhar-se à estratégia e ao valor organizacional.

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

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

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
- AWSWell-Architected Labs: habilite tags de alocação de custos geradas pela AWS
- AWSWell-Architected Labs: políticas de tags
- AWSWell-Architected LabsAWS: Biblioteca de consultas CUR

AWSblogs

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

Documentação do AWS

- Usando etiquetas de alocação de custos - AWS Billing and Cost Management e gerenciamento de custos e gerenciamento de custos

- O que são Relatórios de AWS custos e uso da
- AWS Resource Groups Referência da API
- Como posso usar tags de política do IAM para restringir como uma instância do EC2 ou volume do EBS pode ser criado?
- Modelos de atualização mutáveis versus imutáveis

Other (Outros)

- Bryar, C. e Carr, B. (2021). Trabalhando de trás para frente: insights, histórias e segredos de dentro da Amazon. Londres Macmillan.
- AWS CloudFormation Guard (GitHub)

Revisões do documento

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

Alteração	Descrição	Data
Atualização secundária	Atualizações no gerenciamento de identidade	30 de março de 2023
Revisão menor	Referência atualizada no ABAC para recursos individuais.	24 de fevereiro de 2023
Revisão menor	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	6 de fevereiro de 2023
Revisões importantes	Foi adicionada uma referência mais específica para os tipos de recursos suportados pela regra AWS Config `required_tags` .	18 de janeiro de 2023
Revisões importantes	Atualizado para incluir as práticas e os recursos de serviço mais recentes, especialmente na área de identidade.	29 de setembro de 2022
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	22 de abril de 2022

	e casos de uso. Foram adicionadas mais orientaçõ es prescritivas com base nas ferramentas, técnicas e recursos disponíveis mais recentes.	
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 sua própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não criam nenhum compromisso ou garantia da AWS e de suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte, nem modifica, qualquer contrato entre a AWS e seus clientes.

Glossário do AWS

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