Implementando políticas para permissões de privilégios mínimos para AWS CloudFormation

AWS Orientação prescritiva

AWS Orientação prescritiva: Implementando políticas para permissões de privilégios mínimos para AWS CloudFormation

Table of Contents

Implementando políticas para permissões de privilégios mínimos para AWS CloudFormation

Nima Fotouhi e Moumita Saha, Amazon Web Services (AWS)

Maio de 2023 (histórico do documento)

AWS CloudFormationé um serviço de infraestrutura como código (IaC) que ajuda você a escalar o desenvolvimento de sua infraestrutura de nuvem provisionando recursos AWS . Também ajuda você a gerenciar esses recursos em todo o ciclo de vida, em todos Contas da AWS os sentidos. Regiões da AWS Em CloudFormation, você define modelos, que funcionam como um modelo para um conjunto de recursos. Em seguida, você provisiona esses recursos criando e implantando uma pilha, que é um grupo de recursos relacionados que você gerencia como uma única unidade. Você também pode usar CloudFormation para implantar conjuntos de pilhas, que são grupos de pilhas que você pode criar, atualizar e excluir em várias contas e Regiões da AWS com uma única operação. Este guia fornece uma visão geral de como você pode implementar permissões de privilégios mínimos AWS CloudFormation e recursos provisionados por meio dele. CloudFormation

Você pode implantar CloudFormation pilhas ou conjuntos de pilhas fazendo o seguinte:

- Acesse diretamente o AWS ambiente por meio de um principal AWS Identity and Access Management (IAM) e implante CloudFormation pilhas.
- Coloque as CloudFormation pilhas em um pipeline de implantação e inicie a implantação da pilha por meio do pipeline. O pipeline acessa o AWS ambiente por meio de um diretor do IAM e implanta as pilhas. Essa abordagem é uma prática recomendada.

Para qualquer uma dessas abordagens, são necessárias permissões para implantar CloudFormation pilhas. Por exemplo, considere um usuário planejando usar CloudFormation para criar uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Essa instância exigiria um perfil de instância do IAM para acessar outra Serviços da AWS. O principal do IAM usado para implantar a CloudFormation pilha exigiria as seguintes permissões:

- Permissões para acessar CloudFormation
- Permissões para criar pilhas em CloudFormation
- Permissões para criar instâncias no Amazon EC2

- Permissões para criar os perfis de instância necessários do IAM

O que é privilégio mínimo?

Privilégio mínimo é a prática recomendada de segurança para conceder as permissões mínimas necessárias para executar uma tarefa. O princípio do menor privilégio faz parte do pilar de segurança no Well-Architected AWS Framework. Quando você implementa essa prática recomendada, ela pode ajudar a proteger seu AWS ambiente contra riscos de escalonamento de privilégios, reduzir a superfície de ataque, melhorar a segurança dos dados e evitar erros do usuário (como configurar incorretamente ou excluir um recurso por engano).

Para implementar o menor privilégio para seus AWS recursos, você configura políticas, como políticas baseadas em identidade no AWS Identity and Access Management (IAM). Essas políticas definem as permissões e especificam as condições de acesso. As organizações podem começar com políticas AWS gerenciadas, mas geralmente criam políticas personalizadas que limitam o escopo das permissões somente às ações necessárias para a carga de trabalho ou o caso de uso.

Permissões de privilégio mínimo para o CloudFormation serviço são uma consideração de segurança importante. Como os usuários e desenvolvedores que interagem com eles CloudFormation podem ter a capacidade de criar, modificar ou excluir recursos rapidamente em grande escala, o privilégio mínimo é especialmente essencial. No entanto, CloudFormation requer as permissões necessárias para criar, atualizar e modificar recursos no seu Contas da AWS. Você deve equilibrar a necessidade de permissões para operar CloudFormation com o princípio do menor privilégio.

Ao aplicar o princípio do menor privilégio a CloudFormation, você precisa considerar o seguinte:

- Permissões para o CloudFormation serviço — quais usuários precisam de acesso CloudFormation, qual nível de acesso eles precisam e quais ações eles podem realizar para criar, atualizar ou excluir pilhas?
- Permissões para provisionar recursos — Por meio de quais recursos os usuários podem provisionar CloudFormation?
- Permissões para recursos provisionados — Como você configura as permissões de privilégio mínimo para os recursos por meio dos quais você provisiona? CloudFormation

Resultados de negócios desejados

Seguindo as recomendações e práticas recomendadas deste guia, você pode:

- Determine quais usuários da sua organização precisam de acesso e CloudFormation, em seguida, configure as permissões de privilégio mínimo para esses usuários.
- Use políticas de pilha para ajudar a proteger as CloudFormation pilhas de atualizações não intencionais.
- Configure permissões de privilégios mínimos para CloudFormation usuários e recursos para ajudar a evitar o aumento de privilégios e o problema confuso dos deputados.
- Use AWS CloudFormation para provisionar AWS recursos com permissões de privilégio mínimo. Isso ajuda sua organização a manter uma postura de segurança mais robusta.
- Reduzir proativamente o tempo, a energia e o dinheiro necessários para investigar e mitigar incidentes de segurança.

Público-alvo

Este guia é destinado a arquitetos de infraestrutura de nuvem, DevOps engenheiros e engenheiros de confiabilidade de sites (SREs) que gerenciam e provisionam recursos usando CloudFormation.

Usando políticas de acesso para conceder permissões em AWS

Você gerencia o acesso AWS criando políticas baseadas em identidade e anexando-as aos diretores AWS Identity and Access Management (IAM), como funções ou usuários, e criando políticas baseadas em recursos e anexando-as aos recursos. AWS AWS avalia essas políticas sempre que uma solicitação é feita. As permissões nas políticas determinam se a solicitação será permitida ou negada.

Para entender como configurar o acesso com privilégio mínimo nas políticas, você precisa entender os diferentes tipos de políticas, os elementos e a estrutura de uma política, e como as políticas são avaliadas. Este guia se concentra apenas em políticas baseadas em identidade e em recurso. No entanto, AWS fornece outros tipos de políticas, como políticas de controle de serviço (SCPs), limites de permissões e políticas de sessão. Cada tipo de política desempenha um papel na implementação de permissões de privilégio mínimo em seu. Contas da AWS Para obter mais informações, consulte Políticas e permissões e Aplicar permissões de privilégio mínimo na documentação do IAM.

Configurando permissões de privilégio mínimo a serem usadas CloudFormation

Este capítulo analisa as opções para configurar permissões para acessar e usar o serviço do AWS CloudFormation .

Quando um usuário ou serviço provisiona AWS recursos CloudFormation, a primeira etapa é fazer uma chamada para o CloudFormation serviço por meio de um diretor AWS Identity and Access Management (IAM). Esse diretor do IAM deve ter permissões para criar as CloudFormation pilhas. Em seguida, o diretor do IAM usa uma das seguintes abordagens para provisionar recursos por meio de CloudFormation:

- Se o diretor do IAM não passar as operações da pilha para uma função de CloudFormation serviço, CloudFormation usa as credenciais do diretor do IAM para realizar as operações da pilha. Esse é o padrão. Portanto, além das permissões para realizar as operações de CloudFormation pilha, o diretor do IAM também precisa de permissões para provisionar os recursos definidos nos CloudFormation modelos que eles usarão. Por exemplo, se o diretor do IAM não tiver permissões para criar instâncias do Amazon Elastic Compute Cloud (Amazon EC2), ele não poderá criar CloudFormation uma pilha que provisionaria uma instância do Amazon EC2.
- Se o diretor do IAM passar as operações da pilha para uma função de CloudFormation serviço, CloudFormation usará a função de serviço para realizar as operações da pilha e provisionar os recursos no CloudFormation modelo. Essa função CloudFormation de serviço deve ser definida com permissões para Serviços da AWS provisioná-la em nome do diretor do IAM. Essa abordagem evita dar permissões diretas ao diretor do IAM para provisionar os AWS recursos definidos nos CloudFormation modelos. O diretor do IAM precisa de permissões de criação da CloudFormation pilha e CloudFormation usa a política da função de serviço para fazer chamadas em vez da política do diretor do IAM.

Usando a abordagem da função de serviço e o princípio do privilégio mínimo, você pode padronizar o provisionamento de recursos em seu AWS ambiente e exigir que os usuários provisionem recursos de acordo com a IaC. CloudFormation Como as políticas anexadas aos diretores do IAM não contêm permissões para provisionar AWS recursos diretamente, os usuários devem usá-las CloudFormation para provisioná-las.

Este capítulo analisa os seguintes mecanismos para configurar e gerenciar o acesso ao CloudFormation serviço e às CloudFormation pilhas:

- Políticas baseadas em identidade para CloudFormation— Use esse tipo de política para configurar quais diretores do IAM podem acessar CloudFormation e quais ações eles podem realizar. CloudFormation
- Funções de serviço para CloudFormation— Crie uma função de serviço que permita CloudFormation criar, atualizar ou excluir recursos da pilha em nome do diretor do IAM que implanta a pilha. O perfil de serviço é criado no IAM e pode ser associado a uma ou mais pilhas.
- CloudFormation políticas de pilha: use este tipo de política para determinar quando uma pilha pode ser atualizada. Esse tipo de política pode ajudar a impedir que a pilha de recursos seja involuntariamente atualizada ou excluída. As políticas de pilha são criadas e associadas às pilhas em. CloudFormation

Políticas baseadas em identidade para CloudFormation

Considere os tipos de usuários que precisam AWS CloudFormation acessar e quais ações esses usuários precisam realizar CloudFormation. Você configura as permissões do usuário por meio de políticas baseadas em identidade, que você anexa a um principal AWS Identity and Access Management (IAM), como uma função ou usuário.

Quando você configura uma política baseada em identidade, os elementos `Effect`, `Action` e `Resource` são obrigatórios. Opcionalmente, você também pode definir um elemento `Condition`. Para obter mais informações sobre esses elementos, consulte Referência de elementos de política JSON do IAM.

Esta seção contém os seguintes tópicos:

- Melhores práticas para configurar políticas baseadas em identidade para acesso com privilégios mínimos CloudFormation
- Exemplos de políticas baseadas em identidade para CloudFormation

Melhores práticas para configurar políticas baseadas em identidade para acesso com privilégios mínimos CloudFormation

- Para diretores do IAM que precisam de permissões de acesso CloudFormation, você deve equilibrar a necessidade de permissões para operar CloudFormation com o princípio do menor privilégio. Para ajudar você a aderir ao princípio do privilégio mínimo, recomendamos que defina a entidade principal baseada em identidade do IAM com ações específicas que permitam que a entidade principal faça o seguinte:
  - Crie, atualize e exclua uma CloudFormation pilha.
  - Passe uma ou mais funções de serviço que tenham as permissões necessárias para implantar os recursos definidos nos CloudFormation modelos. Isso permite assumir CloudFormation a função de serviço e provisionar os recursos na pilha em nome do diretor do IAM.
- O escalonamento de privilégios refere-se à capacidade de um usuário com acesso elevar seus níveis de permissão e comprometer a segurança. O privilégio mínimo é uma prática recomendada importante que pode ajudar a evitar o escalonamento de privilégios. Como CloudFormation oferece suporte ao provisionamento de tipos de recursos do IAM, como políticas e funções, um diretor do IAM pode escalar seus privilégios da seguinte forma: CloudFormation
  - Usar uma CloudFormation pilha para provisionar um diretor do IAM com permissões, políticas ou credenciais altamente privilegiadas — Para ajudar a evitar isso, recomendamos o uso de proteções de permissão para restringir o nível de acesso dos diretores do IAM. As barreiras de proteção de permissões definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade principal do IAM. Isso ajuda a evitar o aumento intencional e não intencional de privilégios. Você pode usar os seguintes tipos de políticas como barreiras de proteção de permissões:
    - Os limites de permissões definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade principal do IAM. Para obter mais informações, consulte Limites de permissões para entidades do IAM.
    - Em AWS Organizations, você pode usar políticas de controle de serviço (SCPs) para definir o máximo de permissões disponíveis em um nível organizacional. SCPs afetam somente funções e usuários do IAM que são gerenciados por contas na organização. Você pode SCPs anexar a contas, unidades organizacionais ou à raiz organizacional. Para obter mais informações, consulte Efeitos do SCP sobre as permissões.

- Criação CloudFormation de uma função de serviço que ofereça permissões abrangentes — Para ajudar a evitar isso, recomendamos que você adicione as seguintes permissões refinadas às políticas baseadas em identidade para diretores do IAM que usarão: CloudFormation
  - Use a chave de `cloudformation:RoleARN` condição para controlar quais funções CloudFormation de serviço o diretor do IAM pode usar.
  - Permita a `iam:PassRole` ação somente para as funções CloudFormation de serviço específicas que o diretor do IAM precisa passar.

  Para obter mais informações, consulte Conceder permissões principais ao IAM para usar uma função de CloudFormation serviço neste guia.
- Restrinja as permissões usando proteções de permissões, como limites de permissões e SCPs, e conceda permissões usando uma política baseada em identidade ou em recursos.

Exemplos de políticas baseadas em identidade para CloudFormation

Esta seção contém exemplos de políticas baseadas em identidade que demonstram como conceder e negar permissões para. CloudFormation Você pode usar esses exemplos de políticas para começar a projetar suas próprias políticas que sigam o princípio de privilégio mínimo.

Para obter uma lista de ações e condições CloudFormation específicas, consulte Ações, recursos e chaves de condição para AWS CloudFormation e AWS CloudFormation condições. Para obter uma lista dos tipos de recursos para usar com condições, consulte Referência de tipos de propriedades e recursos da AWS.

Esta seção contém os seguintes exemplos de políticas:

- Permitir acesso às visualizações
- Permitir a criação de pilhas com base no modelo
- Negar a atualização ou exclusão de uma pilha

Permitir acesso às visualizações

O acesso à visualização é o tipo de acesso menos privilegiado a. CloudFormation Esse tipo de política pode ser apropriado para os diretores do IAM que desejam visualizar todas as CloudFormation pilhas no. Conta da AWS O exemplo de política a seguir concede permissões para visualizar os detalhes de qualquer CloudFormation pilha na conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Permitir a criação de pilhas com base no modelo

O exemplo de política a seguir permite que os diretores do IAM criem pilhas usando somente os CloudFormation modelos armazenados em um bucket específico do Amazon Simple Storage Service (Amazon S3). O nome de um bucket é `my-CFN-templates`. Você pode carregar modelos aprovados para esse bucket. A chave de condição `cloudformation:TemplateUrl` na política impede que a entidade principal do IAM use qualquer outro modelo para criar pilhas.

> **Important**
>
> Permita que a entidade principal do IAM tenha acesso somente leitura a esse bucket do S3. Isso ajuda a impedir que a entidade principal do IAM adicione, remova ou modifique os modelos aprovados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringLike": {
          "cloudformation:TemplateUrl": "https:// my-CFN-templates.s3.amazonaws.com/*"
        }
      }
    }
  ]
}
```

Negar a atualização ou exclusão de uma pilha

Para ajudar a proteger CloudFormation pilhas específicas que provisionam AWS recursos essenciais para os negócios, você pode restringir as ações de atualização e exclusão dessa pilha específica. Você pode permitir essas ações somente para algumas entidades principais do IAM especificadas e negá-las para qualquer outra entidade principal do IAM no ambiente. A declaração de política a seguir nega permissões para atualizar ou excluir uma CloudFormation pilha específica em um e. Região da AWS Conta da AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>"
    }
  ]
}
```

Esta declaração de política nega permissões para atualizar ou excluir a `MyProductionStack` CloudFormation pilha, que está no `us-east-1` Região da AWS e no. `123456789012` Conta da AWS Você pode ver o ID da pilha no CloudFormation console. Confira abaixo alguns exemplos de como modificar o elemento `Resource` dessa instrução para seu caso de uso:

- Você pode adicionar várias CloudFormation pilhas IDs no `Resource` elemento dessa política.

- Você pode usar `arn:aws:cloudformation:us-east-1:123456789012:stack/*` para impedir que os principais do IAM atualizem ou excluam qualquer pilha que esteja na `us-east-1` Região da AWS e na conta. `123456789012`

Uma etapa importante é decidir qual política deve conter essa instrução. Você pode adicionar essa instrução às seguintes políticas:

- A política baseada em identidade anexada ao diretor do IAM — colocar a declaração nessa política impede que o diretor específico do IAM crie ou exclua uma pilha específica. CloudFormation
- Um limite de permissões vinculado à entidade principaldo IAM: colocar a instrução nessa política cria uma barreira de proteção de permissão. Ela impede que mais de um principal do IAM crie ou exclua uma CloudFormation pilha específica, mas não restringe todos os principais em seu ambiente.
- Um SCP anexado a uma conta, unidade organizacional ou organização: colocar a instrução nessa política cria uma barreira de proteção de permissão. Ela impede que todos os diretores do IAM na conta, unidade organizacional ou organização de destino criem ou excluam uma pilha específica. CloudFormation

  No entanto, se você não permitir que pelo menos um principal do IAM, um principal privilegiado, atualize ou exclua a CloudFormation pilha, você não poderá fazer nenhuma alteração, quando necessário, nos recursos provisionados por meio dessa pilha. Um usuário ou um pipeline de desenvolvimento (recomendado) pode assumir essa entidade principal privilegiada. Se você quiser implantar a restrição como uma SCP, recomendamos a instrução de política a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": [
```

```
            "<ARN of the allowed privilege IAM principal>"
          ]
        }
      }
    }
  ]
}
```

Nessa instrução, o elemento `Condition` define a entidade principal do IAM que é excluída da SCP. Essa declaração nega qualquer permissão principal do IAM para atualizar ou excluir CloudFormation pilhas, a menos que o ARN do IAM principal corresponda ao ARN no elemento. `Condition` A chave de condição `aws:PrincipalARN` aceita uma lista, o que significa que você pode excluir mais de uma entidade principal do IAM das restrições, conforme necessário para seu ambiente. Para um SCP semelhante que impede modificações nos CloudFormation recursos, consulte SCP-CLOUDFORMATION-1 (). GitHub

Funções de serviço para CloudFormation

Uma função de serviço é uma função AWS Identity and Access Management (IAM) que permite AWS CloudFormation criar, atualizar ou excluir recursos da pilha. Se você não fornecer uma função de serviço, CloudFormation use as credenciais do diretor do IAM para realizar as operações de pilha. Se você criar uma função de serviço CloudFormation e especificar a função de serviço durante a criação da pilha, CloudFormation usará as credenciais da função de serviço para realizar as operações, em vez das credenciais do diretor do IAM.

Ao usar uma função de serviço, a política baseada em identidade anexada ao diretor do IAM não exige permissões para provisionar todos os AWS recursos definidos no CloudFormation modelo. Se você não estiver pronto para provisionar AWS recursos para operações comerciais críticas por meio de um pipeline de desenvolvimento (uma prática AWS recomendada), o uso de uma função de serviço pode adicionar uma camada extra de proteção para o gerenciamento de recursos AWS. As vantagens dessa abordagem são:

- Os diretores do IAM em sua organização seguem um modelo de privilégios mínimos que os impede de criar ou alterar AWS manualmente recursos em seu ambiente.
- Para criar, atualizar ou excluir AWS recursos, os diretores do IAM devem usar CloudFormation. Isso padroniza o provisionamento de recursos por meio da infraestrutura como código.

Por exemplo, para criar uma pilha que contenha uma instância do Amazon Elastic Compute Cloud (Amazon EC2), a entidade principal do IAM precisará ter permissões para criar instâncias do EC2 por meio de sua política baseada em identidade. Em vez disso, CloudFormation pode assumir uma função de serviço que tenha permissões para criar instâncias do EC2 em nome do diretor. Com essa abordagem, a entidade principal do IAM pode criar a pilha, e você não precisa conceder à entidade principal do IAM permissões excessivamente amplas para um serviço ao qual ela não deverá ter acesso regular.

Para usar uma função de serviço para criar CloudFormation pilhas, os diretores do IAM devem ter permissões para transmitir a função de serviço CloudFormation, e a política de confiança da função de serviço deve permitir assumir CloudFormation a função.

Esta seção contém os seguintes tópicos:

- Implementando privilégios mínimos para funções CloudFormation de serviço
- Configuração de perfis de serviço
- Conceder permissões principais ao IAM para usar uma função de CloudFormation serviço
- Configurando uma política de confiança para a função CloudFormation de serviço
- Associação de um perfil de serviço a uma pilha

Implementando privilégios mínimos para funções CloudFormation de serviço

Em um perfil de serviço, você define uma política de permissões que especifica explicitamente quais ações o serviço pode realizar. Elas podem não ser as mesmas ações que uma entidade principal do IAM pode realizar. Recomendamos que você trabalhe retroativamente a partir de seus CloudFormation modelos para criar uma função de serviço que siga o princípio do privilégio mínimo.

Definir o escopo adequado da política baseada em identidade de uma entidade principal do IAM para passar somente perfis de serviço específicos e definir o escopo da política de confiança de um perfil de serviço para permitir que somente entidades principais específicas assumam o perfil ajuda a evitar possíveis escalonamentos de privilégios por meio de perfis de serviço.

Configuração de perfis de serviço

> **Note**
>
> Os perfis de serviço são configurados no IAM. Para criar um perfil de serviço, você deve ter as permissões. Um diretor do IAM com permissões para criar uma função e anexar qualquer política pode escalar suas próprias permissões. AWS recomenda criar uma função de serviço AWS service (Serviço da AWS) para cada caso de uso. Depois de criar funções CloudFormation de serviço para seus casos de uso, você pode permitir que os usuários passem somente a função de serviço aprovada para CloudFormation. Para exemplos de políticas baseadas em identidade que permitem aos usuários criar perfis de serviço, consulte Permissões de perfil de serviço na documentação do IAM.

Para obter instruções sobre como criar funções de serviço, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS). Especifique o CloudFormation (`cloudformation.amazonaws.com`) como o serviço que pode assumir a função. Isso impede que uma entidade principal do IAM assuma a função sozinha ou a passe para outros serviços. Quando você configura um perfil de serviço, os elementos `Effect`, `Action` e `Resource` são obrigatórios. Opcionalmente, você também pode definir um elemento `Condition`.

Para obter mais informações sobre esses elementos, consulte Referência de elementos de política JSON do IAM. Para obter uma lista completa de ações, recursos e chaves de condição, consulte Actions, resources, and condition keys for Identity And Access Management.

Conceder permissões principais ao IAM para usar uma função de CloudFormation serviço

Para provisionar recursos CloudFormation usando a função CloudFormation de serviço, o diretor do IAM deve ter permissões para transmitir a função de serviço. Você pode limitar as permissões da entidade principal do IAM para passar somente determinados perfis especificando o ARN do perfil nas permissões dela. Para obter mais informações, consulte Conceder permissões a um usuário para passar um perfil para um AWS service (Serviço da AWS) na documentação do IAM.

A instrução de política baseada em identidade do IAM a seguir permite que a entidade principal passe perfis, incluindo perfis de serviço, que estão no caminho `cfnroles`. A entidade principal não pode passar perfis que estejam em um caminho diferente.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/cfnroles/*"
}
```

Outra abordagem para limitar os diretores a determinadas funções é usar um prefixo para nomes de funções de CloudFormation serviço. A instrução de política a seguir permite que as entidades principais do IAM passem somente perfis que tenham um prefixo `CFN-`.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/CFN-*"
}
```

Além das instruções de política anteriores, você pode usar a chave de condição `cloudformation:RoleARN` para fornecer mais controles refinados na política baseada em identidade, para obter acesso com privilégio mínimo. A declaração de política a seguir permite que o diretor do IAM crie, atualize e exclua pilhas somente se elas passarem por uma função de CloudFormation serviço específica. Como variação, você pode definir a ARNs de mais de uma função CloudFormation de serviço na chave de condição.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringEquals": {
      "cloudformation:RoleArn": [
        "<ARN of the specific CloudFormation service role>"
      ]
    }
```

```
  }
}
```

Além disso, você também pode usar a chave de `cloudformation:RoleARN` condição para impedir que um diretor do IAM transmita uma função de CloudFormation serviço altamente privilegiada para operações de pilha. A única alteração necessária é no operador condicional, de `StringEquals` para `StringNotEquals`.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringNotEquals": {
      "cloudformation:RoleArn": [
        "<ARN of a privilege CloudFormation service role>"
      ]
    }
  }
}
```

Configurando uma política de confiança para a função CloudFormation de serviço

Uma política de confiança de um perfil é uma política baseada em recurso necessária anexada a um perfil do IAM. A política de confiança define quais entidades principais do IAM podem assumir o perfil. Em uma política de confiança, você pode especificar usuários, perfis, contas ou serviços como entidades principais. Para evitar que os diretores do IAM passem funções de serviço CloudFormation para outros serviços, você pode especificar CloudFormation como principal na política de confiança da função.

A política de confiança a seguir permite que somente o CloudFormation serviço assuma a função de serviço.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudformation.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

Associação de um perfil de serviço a uma pilha

Depois que um perfil de serviço for criado, você poderá associá-lo a uma pilha ao criá-la. Para obter mais informações, consulte Configurar opções de pilha. Antes de especificar um perfil de serviço, certifique-se de que as entidades principais do IAM tenham as permissões para passá-lo. Para obter mais informações, consulte Conceder permissões principais ao IAM para usar uma função de CloudFormation serviço.

CloudFormation políticas de pilha

As políticas de pilha podem ajudar a impedir que os recursos de pilha sejam involuntariamente atualizados ou excluídos durante uma atualização da pilha. Uma política de pilha é um documento JSON que define quais ações de atualização podem ser executadas nos recursos designados. Por padrão, qualquer diretor do IAM com `cloudformation:UpdateStack` permissões pode atualizar todos os recursos em uma AWS CloudFormation pilha. As atualizações podem causar interrupções ou podem excluir e substituir completamente os recursos. Você pode usar uma política de pilha para ajudar a configurar permissões com privilégio mínimo. As políticas de pilha podem fornecer uma camada extra de proteção.

Por padrão, uma política de pilha ajuda a proteger todos os recursos na pilha. No entanto, o principal benefício das políticas de pilha é que elas fornecem controle granular para cada AWS recurso implantado em uma pilha. CloudFormation Você pode usar uma política de pilha para ajudar a proteger somente recursos específicos em uma pilha e permitir atualizações ou a exclusão de outros recursos na mesma pilha. Para permitir atualizações em recursos específicos, você inclui uma instrução `Allow` explícita para esses recursos em sua política de pilha.

As políticas de pilha fornecem controles preventivos para as CloudFormation pilhas às quais estão anexadas. Cada pilha pode ter somente uma política de pilha, mas você pode usar essa política de

pilha para ajudar a proteger todos os recursos dentro dessa pilha. Você pode aplicar uma política de pilha a várias pilhas.

Por exemplo, imagine que você tenha um pipeline que produz artefatos sensíveis e os armazena em um bucket do Amazon Simple Storage Service (Amazon S3) temporariamente para processamento adicional. O bucket S3 é provisionado por CloudFormation, e todos os controles de segurança necessários estão em vigor. Sem políticas de pilha, um desenvolvedor pode alterar intencionalmente ou não o destino dos artefatos do pipeline para um bucket S3 menos seguro e expor dados sensíveis. Se você tiver uma política de pilha aplicada à pilha, ela impedirá que usuários autorizados realizem ações indesejadas de atualização ou exclusão.

Esta seção contém os seguintes tópicos:

- Configuração de políticas de pilha
- Definição e substituição de políticas de pilha
- Limitação e exigência de políticas de pilha

Configuração de políticas de pilha

Quando você configura um perfil de pilha, os elementos `Effect`, `Action`, `Principal` e `Resource` são obrigatórios. Opcionalmente, você também pode definir um elemento `Condition`.

Quando você cria uma política de pilha, por padrão, ela impede atualizações em todos os recursos na pilha. Você personaliza a política de pilha para definir quais ações são explicitamente permitidas. Se quiser inverter a política, você pode definir uma instrução `Allow` que permita todas as ações e, em seguida, especificar instruções `Deny` explícitas que impeçam as ações somente em recursos específicos. Para referência, consulte este exemplo de política de pilha na CloudFormation documentação.

Para obter mais informações sobre o uso desses elementos para criar políticas de pilha personalizadas e mais exemplos de políticas, consulte Definindo uma política de pilha e Mais exemplos de políticas de pilha na documentação. CloudFormation

Definição e substituição de políticas de pilha

Depois de criar uma política de pilha, você a associa a uma pilha. Se você estiver atribuindo a política de pilha a uma pilha existente, deverá usar o AWS Command Line Interface ().AWS CLI No entanto, se você estiver atribuindo a política no momento da criação da pilha, poderá usar o

CloudFormation console ou o. AWS CLI Para obter instruções, consulte Como definir uma política de pilha na CloudFormation documentação.

Quando você quiser permitir que os usuários atualizem ou excluam os recursos na pilha, você precisa substituir temporariamente a política da pilha. Esta substituição permite que você execute ações que de outra forma seriam negadas nos recursos protegidos nessa pilha. Para obter instruções, consulte Atualização de recursos protegidos na CloudFormation documentação.

Limitação e exigência de políticas de pilha

Como prática recomendada para permissões com privilégio mínimo, considere exigir que as entidades principais do IAM atribuam políticas de pilha e limitar quais políticas de pilha as entidades principais do IAM podem atribuir. Muitas entidades principais do IAM não devem ter permissões para criar e atribuir políticas de pilha personalizadas às suas próprias pilhas.

Depois de criar suas políticas de pilha, recomendamos que as carregue em um bucket do S3. Em seguida, você pode referenciar essas políticas de pilha usando a chave de condição `cloudformation:StackPolicyUrl` e fornecendo a URL da política de pilha no bucket do S3.

Concessão de permissões para anexar políticas de pilha

Como prática recomendada para permissões com privilégios mínimos, considere limitar quais políticas de pilha os diretores do IAM podem anexar às pilhas. CloudFormation Na política baseada em identidade para a entidade principal do IAM, você pode especificar quais políticas de pilha a entidade principal do IAM tem permissões para atribuir. Isso impede que a entidade principal do IAM anexe qualquer política de pilha, o que pode reduzir o risco de configuração incorreta.

Por exemplo, uma organização pode ter equipes diferentes com requisitos diferentes. Assim, cada equipe cria políticas de pilha para suas pilhas específicas. CloudFormation Em um ambiente compartilhado, se todas as equipes armazenarem suas políticas de pilha no mesmo bucket do S3, um membro da equipe poderá anexar uma política de pilha disponível, mas não destinada às pilhas da equipe. CloudFormation Para evitar esse cenário, você pode definir uma instrução de política que permita que as entidades principais do IAM anexem somente políticas de pilha específicas.

O exemplo de política a seguir permite que a entidade principal do IAM anexe políticas de pilha que são armazenadas em uma pasta específica da equipe em um bucket do S3. Você pode armazenar políticas de pilha aprovadas nesse bucket.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:StackPolicyUrl": "<Bucket URL>/<Team folder>/*"
        }
      }
    }
  ]
}
```

Essa instrução de política não exige que uma entidade principal do IAM atribua uma política de pilha a cada pilha. Mesmo que a entidade principal do IAM tenha permissões para criar pilhas com uma política de pilha específica, ele pode optar por criar uma pilha que não tenha uma política de pilha.

Exigência de políticas de pilha

Para garantir que todas as entidades principais do IAM atribuam políticas de pilha às suas pilhas, você pode definir uma política de controle de serviços (SCP) ou um limite de permissões como uma barreira de proteção preventiva.

O exemplo de política a seguir mostra como você pode configurar uma SCP que exija que as entidades principais do IAM atribuam uma política de pilha ao criar uma pilha. Se a entidade principal do IAM não anexar uma política de pilha, ela não poderá criar a pilha. Além disso, essa política impede que entidades principais do IAM com permissões de atualização de pilha removam a política de pilha durante uma atualização. A política restringe a ação `cloudformation:UpdateStack` usando a chave de condição `cloudformation:StackPolicyUrl`.

```
        {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
```

```
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:StackPolicyUrl": "true"
        }
      }
    }
  ]
}
```

Ao incluir essa instrução de política em uma SCP em vez de um limite de permissões, você pode aplicar sua barreira de proteção a todas as contas da organização. Isso pode fazer o seguinte:

1. Reduzir o esforço de anexar a política individualmente a várias entidades principais do IAM em uma Conta da AWS. Os limites de permissões só podem ser anexados diretamente a uma entidade principal do IAM.
2. Reduzir o esforço de criar e gerenciar várias cópias do limite de permissões para diferentes Contas da AWS. Isso reduz o risco de erro de configuração em vários limites de permissões idênticos.

> **Note**
>
> SCPs e os limites de permissões são barreiras de permissões que definem o máximo de permissões disponíveis para diretores do IAM em uma conta ou organização. Essas políticas não concedem permissões às entidades principais do IAM. Se você quiser padronizar a exigência de que todas as entidades principais do IAM em sua conta ou organização atribuam políticas de pilha, você precisa usar tanto as barreiras de proteção de permissão quanto as políticas baseadas em identidade.

Configurando permissões de privilégio mínimo para recursos provisionados por meio de CloudFormation

AWS CloudFormation permite provisionar vários tipos diferentes de AWS recursos. Os recursos provisionados exigem seu próprio conjunto de permissões para funcionar conforme o esperado e para configurar quem tem acesso a esses recursos. O capítulo anterior analisou as opções para configurar permissões para acessar e usar o CloudFormation serviço. Este capítulo analisa como você pode aplicar o princípio do menor privilégio aos recursos provisionados por meio de. CloudFormation

Neste guia, seria praticamente impossível revisar as recomendações de segurança e as melhores práticas para cada tipo de AWS recurso que pode ser provisionado. CloudFormation Se você tiver dúvidas relacionadas a um serviço específico, recomendamos revisar a documentação desse serviço. A maioria dos AWS service (Serviço da AWS) documentos contém uma seção de segurança e informações sobre as permissões necessárias para usar esse serviço. Para obter uma lista completa da documentação de AWS service (Serviço da AWS) , consulte a documentação da AWS.

A seguir estão as etapas de alto nível, independentes de serviços, que você pode seguir para criar CloudFormation modelos que sigam o princípio do privilégio mínimo:

1. Prepare uma lista dos recursos que você planeja provisionar usando CloudFormation.
2. Consulte a documentação da AWS dos serviços correspondentes e revise as seções sobre segurança e gerenciamento de acesso. Isso ajuda a compreender as recomendações e os requisitos específicos do serviço.
3. Use as informações coletadas nas etapas anteriores para criar CloudFormation modelos e políticas associadas que permitam somente as permissões necessárias e neguem todas as outras.

A seguir, este guia analisa um exemplo de como você pode aplicar o princípio do privilégio mínimo em CloudFormation modelos, usando um caso de uso real.

Exemplo: bucket do Amazon S3 para armazenar artefatos de um pipeline

Este exemplo cria um bucket do Amazon Simple Storage Service (Amazon S3) que é usado para armazenar artefatos do projeto do AWS CodeBuild. O AWS CodePipeline usa esses artefatos armazenados. Você pode permitir CodeBuild e CodePipeline acessar esse bucket do S3 por meio de funções de serviço e controlar esse acesso usando uma política de bucket do Amazon S3. Confira abaixo os nomes dos recursos usados neste exemplo:

- `Deployfiles_build`é o nome do CodeBuild projeto.
- `Deployment-Pipeline`é o nome do pipeline em CodePipeline.

Definir o bucket do Amazon S3

Primeiro, você define o bucket do S3 no CloudFormation modelo, que é um arquivo de texto formatado em YAML.

```
amzn-s3-demo-bucket:
  Type: AWS::S3::Bucket
  Properties:
    PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

Definir a política de bucket do Amazon S3

Em seguida, no CloudFormation modelo, você cria uma política de bucket que permite que somente o `Deployfiles_build` projeto e o `Deployment-Pipeline` pipeline acessem o bucket.

```
MyBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref amzn-s3-demo-bucket
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
```

```
      - Sid: "S3ArtifactRepoAccess"
        Effect: Allow
        Action:
          - 's3:GetObject'
          - 's3:GetObjectVersion'
          - 's3:PutObject'
          - 's3:GetBucketVersioning'
        Resource:
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}'
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}/*'
        Principal:
          Service:
            - codebuild.amazonaws.com
            - codepipeline.amazonaws.com
        Condition:
          StringLike:
            'aws:SourceArn':
              - !Sub 'arn:aws:codebuild:${AWS::Region}:${AWS::AccountId}:project/
Deployfiles_build'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline/*'
```

Observe o seguinte sobre essa política de bucket:

- O elemento `Resource` lista dois tipos diferentes de recursos que usam os seguintes formatos de nome do recurso da Amazon (ARN):
  - O formato ARN de um objeto do S3 é `arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*`/$`*`<ObjectName>`*.
  - O formato ARN de um bucket do S3 é `arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*.

  `s3:GetObject`, `s3:GetObjectVersion` e `s3:PutObject` exigem um tipo de recurso de objeto S3 e `s3:GetBucketVersioning` requer um tipo de recurso de bucket do S3. Para obter mais informações sobre os tipos de recursos necessários para cada ação, consulte Ações, recursos e chaves de condição do Amazon S3.
- O elemento `Principal` lista as entidades que têm permissão para realizar as ações do Amazon S3 definidas na declaração. Nesse caso, somente CodeBuild e CodePipeline estão autorizados a realizar essas ações.

- O `Condition` elemento restringe ainda mais o acesso ao bucket do S3 para que somente o `Deployfiles_build` CodeBuild projeto, o `Deployment-Pipeline` CodePipeline pipeline e as ações do pipeline possam acessar o bucket.

Criar os perfis de serviço

Embora a política do bucket controle o acesso ao bucket, ela não concede permissões para CodeBuild e CodePipeline para acessá-lo. Para conceder acesso, você precisa criar um perfil de serviço para cada serviço e adicionar a declaração a seguir a cada um. Os serviços funcionam CodeBuild e CodePipeline permitem que os serviços acessem o bucket do S3 e seus objetos.

```
Sid: "ViewAccessToS3ArtifactRepo"
Effect: Allow
Action:
  - ‘s3:GetObject'
  - ‘s3:GetObjectVersion'
  - ‘s3:PutObject'
  - ‘s3:GetBucketVersioning'
Resource:
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}'
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}/*'
```

Melhores práticas para permissões com privilégios mínimos para AWS CloudFormation

Este guia analisa diferentes abordagens e alguns tipos de políticas que você pode usar para configurar o acesso com privilégios mínimos AWS CloudFormation e os recursos provisionados por meio deles. CloudFormation Este guia se concentra na configuração do acesso CloudFormation por meio de diretores, funções de serviço e políticas de pilha do IAM. As recomendações e as práticas recomendadas incluídas foram criadas para ajudar a proteger suas contas e recursos de pilha contra ações não intencionais de usuários autorizados e de agentes mal-intencionados que possam explorar permissões excessivas.

Veja a seguir um resumo das práticas recomendadas explicadas neste guia. Essas melhores práticas podem ajudá-lo a aderir ao princípio do privilégio mínimo ao configurar permissões de uso CloudFormation e recursos provisionados por meio de: CloudFormation

- Determine o nível de acesso que os usuários e as equipes precisam para usar o CloudFormation serviço e conceda somente o acesso mínimo necessário. Por exemplo, conceda acesso de visualização a estagiários e auditores e não permita que esses tipos de usuários criem, atualizem ou excluam pilhas.
- Para diretores do IAM que precisam provisionar vários tipos de AWS recursos por meio de CloudFormation pilhas, considere usar funções de serviço CloudFormation para permitir o provisionamento de recursos em nome do diretor, em vez de configurar o acesso às políticas baseadas Serviços da AWS em identidade do diretor.
- Nas políticas baseadas em identidade para diretores do IAM, use a chave de `cloudformation:RoleARN` condição para controlar quais funções de CloudFormation serviço podem ser passadas.
- Para ajudar a evitar a escalada de privilégios, faça o seguinte:
  - Monitore rigorosamente todos os diretores do IAM que têm acesso ao CloudFormation serviço e os níveis de acesso que eles têm.
  - Monitore rigorosamente quais usuários podem acessar essas entidades principais do IAM.
  - Monitore a atividade dos diretores do IAM que podem passar uma função de serviço privilegiada para o. CloudFormation Embora elas possam não ter permissões para criar recursos do IAM por meio de sua política baseada em identidade, o perfil de serviço que elas podem transmitir pode criar recursos do IAM.

- Especifique uma política de pilha sempre que criar uma pilha com recursos críticos. Isso pode ajudar a proteger recursos de pilha críticos contra atualizações não intencionais capazes de fazer com que os recursos sejam interrompidos ou até mesmo substituídos.
- Para recursos provisionados por meio de CloudFormation, consulte as recomendações de gerenciamento de acesso e as melhores práticas de segurança para esse serviço.
- Para complementar as recomendações deste guia para políticas baseadas em identidade e políticas baseadas em recursos, considere a implementação de controles de segurança adicionais para permissões de privilégios mínimos, como políticas de controle de serviço () e limites de permissões. SCPs Para obter mais informações, consulte Próximas etapas.

A CloudFormation documentação contém práticas recomendadas e práticas recomendadas de segurança adicionais que podem ajudar você a usar com CloudFormation mais eficiência e segurança. Além disso, consulte Melhores práticas para configurar políticas baseadas em identidade para acesso com privilégios mínimos CloudFormation neste guia.

Próximas etapas

Você pode usar as informações e os exemplos deste guia para começar a aplicar o princípio de privilégio mínimo em sua organização. Recomendamos que você revise os recursos adicionais na seção Recursos, que contém referências de documentação e ferramentas que podem ajudar você a refinar suas políticas.

Este guia tem como objetivo ajudar você a começar a implementar o acesso com privilégio mínimo para o AWS CloudFormation. No entanto, existem outros tipos de políticas que podem ajudar a fortalecer o princípio do privilégio mínimo em sua organização. Com base em seu ambiente e nos requisitos de negócios, talvez você queira implementar controles adicionais que não são analisados neste guia. Como próxima etapa e para obter mais informações, recomendamos que você revise os seguintes tópicos relacionados ao privilégio mínimo e à configuração de acesso e permissões:

- Limites de permissões para entidades do IAM
- Políticas de controle de serviços (SCP)
- Funções para acesso entre contas
- Federação de identidades
- Visualização das informações acessadas pela última vez para o IAM

As ferramentas a seguir podem ajudar você a monitorar o acesso e as permissões com privilégio mínimo para o CloudFormation:

- AWS Identity and Access Management Access Analyzer
- Você pode usar a guia Consultor de acesso no console do AWS Identity and Access Management (IAM) para identificar permissões excessivas para identidades do IAM. Por exemplo, consulte Tighten S3 permissions for your IAM users and roles using access history of S3 actions (publicação do Blog da AWS).
- Você pode usar uma ferramenta de análise de código, como cfn-policy-validator (GitHub), para ajudar a identificar permissões excessivas.

Quando você estiver confortável com a criação e o gerenciamento de permissões do CloudFormation, é recomendável usar pipelines de integração e entrega contínuas (CI/CD) para implantar seus modelos do CloudFormation. Isso reduz o risco de erros humanos e torna o processo de implantação mais rápido.

Recursos

AWS CloudFormation documentação

- Controlando o acesso com AWS Identity and Access Management
- AWS referência de tipos de recursos e propriedades
- Configuração das opções de pilha do AWS CloudFormation
- AWS CloudFormation função de serviço

AWS Identity and Access Management Documentação (IAM)

- Políticas e permissões no IAM
- Referência de elementos de política JSON do IAM
- Lógica da avaliação de política
- Serviços da AWS compatíveis com o IAM
- Criação de uma função para delegar permissões a um AWS service (Serviço da AWS)
- O problema de "confused deputy"
- Práticas recomendadas de segurança no IAM

Outras AWS referências

- Ações, recursos e chaves de condição para Serviços da AWS (Referência de autorização do serviço)
- Conceda acesso com privilégios mínimos (AWS Well-Architected Framework)
- Técnicas para escrever políticas de IAM com privilégios mínimos (postagem AWS no blog)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Atualizações significativas	Revisamos e refinamos de forma significativa a orientação e os exemplos de instruções de política para abordar casos de uso organizacional comuns.	5 de maio de 2023
Publicação inicial	—	9 de março de 2023

AWS Glossário de orientação prescritiva

A seguir estão os termos comumente usados em estratégias, guias e padrões fornecidos pela Orientação AWS Prescritiva. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

Números

7 Rs

Sete estratégias comuns de migração para mover aplicações para a nuvem. Essas estratégias baseiam-se nos 5 Rs identificados pela Gartner em 2011 e consistem em:

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Relational Database Service (Amazon RDS) para Oracle na Nuvem AWS.
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migrar seu banco de dados Oracle on-premises para o Oracle em uma instância do EC2 na Nuvem AWS.
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma on-premises para um serviço de nuvem para a mesma plataforma. Exemplo: migrar um Microsoft Hyper-V aplicativo para o. AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de acesso baseado em atributo.

serviços abstraídos

Veja serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia (por meio de uma ferramenta de replicação bidirecional ou operações de gravação dupla), e ambos os bancos de dados lidam com transações de aplicações conectadas durante a migração. Esse método oferece suporte à migração em lotes pequenos e controlados, em vez de exigir uma substituição única. É mais flexível, mas exige mais trabalho do que a migração ativa-passiva.

migração ativa-passiva

Um método de migração de banco de dados em que os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações das aplicações conectadas, enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

AGGREGATE FUNCTION

Uma função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem `SUM` e `MAX`.

AI

Veja inteligência artificial.

AIOps

Veja operações de inteligência artificial.

anonimização

O processo de excluir permanentemente informações pessoais em um conjunto de dados. A anonimização pode ajudar a proteger a privacidade pessoal. Dados anônimos não são mais considerados dados pessoais.

antipadrões

Uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa.

controle de aplicações

Uma abordagem de segurança que permite o uso somente de aplicações aprovadas para ajudar a proteger um sistema contra malware.

portfólio de aplicações

Uma coleção de informações detalhadas sobre cada aplicação usada por uma organização, incluindo o custo para criar e manter a aplicação e seu valor comercial. Essas informações são fundamentais para o processo de descoberta e análise de portfólio e ajudam a identificar e priorizar as aplicações a serem migradas, modernizadas e otimizadas.

inteligência artificial (IA)

O campo da ciência da computação que se dedica ao uso de tecnologias de computação para desempenhar funções cognitivas normalmente associadas aos humanos, como aprender, resolver problemas e reconhecer padrões. Para obter mais informações, consulte O que é inteligência artificial?

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter mais informações sobre como AIOps é usado na estratégia de AWS migração, consulte o guia de integração de operações.

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para descriptografia. É possível compartilhar a chave pública porque ela não é usada na descriptografia, mas o acesso à chave privada deve ser altamente restrito.

atomicidade, consistência, isolamento, durabilidade (ACID)

Um conjunto de propriedades de software que garantem a validade dos dados e a confiabilidade operacional de um banco de dados, mesmo no caso de erros, falhas de energia ou outros problemas.

controle de acesso por atributo (ABAC)

A prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte ABAC AWS na documentação AWS Identity and Access Management (IAM).

fonte de dados autorizada

Um local onde você armazena a versão principal dos dados, que é considerada a fonte de informações mais confiável. Você pode copiar dados da fonte de dados autorizada para outros locais com o objetivo de processar ou modificar os dados, como anonimizá-los, redigi-los ou pseudonimizá-los.

Zona de disponibilidade

Um local distinto dentro de um Região da AWS que está isolado de falhas em outras zonas de disponibilidade e fornece conectividade de rede barata e de baixa latência a outras zonas de disponibilidade na mesma região.

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização

para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

AWS Estrutura de qualificação da carga de trabalho (AWS WQF)

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot malicioso

Um bot destinado a causar disrupção ou danos a indivíduos ou organizações.

BCP

Veja planejamento de continuidade de negócios

gráfico de comportamento

Uma visualização unificada e interativa do comportamento e das interações de recursos ao longo do tempo. É possível usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, chamadas de API suspeitas e ações similares. Para obter mais informações, consulte Dados em um gráfico de comportamento na documentação do Detective.

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também endianness.

classificação binária

Um processo que prevê um resultado binário (uma de duas classes possíveis). Por exemplo, seu modelo de ML pode precisar prever problemas como “Este e-mail é ou não é spam?” ou “Este produto é um livro ou um carro?”

filtro de bloom

Uma estrutura de dados probabilística e eficiente em termos de memória que é usada para testar se um elemento é membro de um conjunto.

blue/green deployment (implantação azul/verde)

Uma estratégia de implantação em que você cria dois ambientes separados, mas idênticos. Você executa a versão atual da aplicação em um ambiente (azul) e a nova versão da aplicação no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Uma aplicação de software que executa tarefas automatizadas na internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como crawlers da web que indexam informações na internet. Outros bots, conhecidos como bots maliciosos, têm como objetivo causar disrupção ou danos a indivíduos ou organizações.

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como bot herder ou operador de bots. Os botnets são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação existente e, em seguida, desenvolver recursos ou corrigir bugs na nova ramificação. Uma ramificação que você cria para gerar um recurso é comumente chamada de ramificação de recurso. Quando o recurso estiver pronto para lançamento, você mesclará a ramificação do recurso de volta com a ramificação principal. Para obter mais informações, consulte Sobre filiais (GitHub documentação).

Acesso de emergência

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implement break-glass procedures nas orientações do AWS Well-Architected.

estratégia brownfield

A infraestrutura existente em seu ambiente. Ao adotar uma estratégia brownfield para uma arquitetura de sistema, você desenvolve a arquitetura de acordo com as restrições dos sistemas e da infraestrutura atuais. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

cache do buffer

A área da memória em que os dados acessados com mais frequência são armazenados.

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

Um plano que aborda o impacto potencial de um evento disruptivo, como uma migração em grande escala, nas operações e permite que uma empresa retome as operações rapidamente.

C

CAF

Veja AWS Cloud Adoption Framework.

implantação canário

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substitui a versão atual por completo.

CCoE

Veja Centro de Excelência da Nuvem.

CDC

Veja captura de dados de alteração.

captura de dados de alterações (CDC)

O processo de rastrear alterações em uma fonte de dados, como uma tabela de banco de dados, e registrar metadados sobre a alteração. É possível usar o CDC para várias finalidades, como auditar ou replicar alterações em um sistema de destino para manter a sincronização.

engenharia do caos

Introduzir intencionalmente falhas ou eventos disruptivos para testar a resiliência de um sistema. Você pode usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estressam suas AWS cargas de trabalho e avaliar sua resposta.

CI/CD

Veja integração e entrega contínuas.

classificação

Um processo de categorização que ajuda a gerar previsões. Os modelos de ML para problemas de classificação predizem um valor discreto. Os valores discretos são sempre diferentes uns dos outros. Por exemplo, um modelo pode precisar avaliar se há ou não um carro em uma imagem.

criptografia no lado do cliente

Criptografia de dados localmente, antes que o alvo os AWS service (Serviço da AWS) receba.

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as publicações CCo E no blog de estratégia Nuvem AWS corporativa.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem é normalmente conectada à tecnologia de computação de borda.

modelo operacional em nuvem

Em uma organização de TI, o modelo operacional usado para criar, amadurecer e otimizar um ou mais ambientes de nuvem. Para obter mais informações, consulte Criar seu modelo operacional de nuvem.

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam ao migrar para a Nuvem AWS:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação — Fazer investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir um CCo E, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog de estratégia Nuvem AWS empresarial. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Veja banco de dados de gerenciamento de configuração.

repositório de código

Um local onde o código-fonte e outros ativos, como documentação, amostras e scripts, são armazenados e atualizados por meio de processos de controle de versão. Os repositórios de nuvem comuns incluem o GitHub ou o Bitbucket Cloud. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

cache frio

Um cache de buffer que está vazio, não está bem preenchido ou contém dados obsoletos ou irrelevantes. Isso afeta a performance porque a instância do banco de dados deve ler da memória principal ou do disco, um processo que é mais lento do que a leitura do cache do buffer.

dados frios

Dados que raramente são acessados e geralmente são históricos. Ao consultar esse tipo de dados, consultas lentas geralmente são aceitáveis. Mover esses dados para níveis ou classes de armazenamento de baixo desempenho e menos caros pode reduzir os custos.

visão computacional (CV)

Um campo de IA que usa machine learning para analisar e extrair informações de formatos visuais, como vídeos e imagens digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Em uma workload, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a workload se torne incompatível e, normalmente, é gradual e não intencional.

banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

pacote de conformidade

Uma coleção de AWS Config regras e ações de remediação que você pode montar para personalizar suas verificações de conformidade e segurança. Você pode implantar um pacote de conformidade como uma entidade única em uma Conta da AWS região ou em uma organização usando um modelo YAML. Para obter mais informações, consulte Pacotes de conformidade na documentação. AWS Config

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. CI/CD é comumente descrito como um pipeline. CI/CD pode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

Dados estacionários em sua rede, por exemplo, dados que estão em um armazenamento.

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

desvio de dados

Uma variação significativa entre os dados de produção e os dados usados para treinar um modelo de ML ou uma alteração significativa nos dados de entrada ao longo do tempo. O desvio de dados pode reduzir a qualidade geral, a precisão e a imparcialidade das previsões do modelo de ML.

dados em trânsito

Dados que estão se movendo ativamente pela sua rede, como entre os recursos da rede.

data mesh

Um framework de arquitetura que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

O princípio de coletar e processar apenas os dados estritamente necessários. Praticar a minimização de dados no Nuvem AWS pode reduzir os riscos de privacidade, os custos e a pegada de carbono de sua análise.

perímetro de dados

Um conjunto de proteções preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte Construindo um perímetro de dados em. AWS

pré-processamento de dados

A transformação de dados brutos em um formato que seja facilmente analisado por seu modelo de ML. O pré-processamento de dados pode significar a remoção de determinadas colunas ou linhas e o tratamento de valores ausentes, inconsistentes ou duplicados.

proveniência dos dados

O processo de rastrear a origem e o histórico dos dados ao longo de seu ciclo de vida, por exemplo, como os dados foram gerados, transmitidos e armazenados.

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados compatível com business intelligence, como analytics. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

Instruções ou comandos para criar ou modificar a estrutura de tabelas e objetos em um banco de dados.

linguagem de manipulação de dados (DML)

Instruções ou comandos para modificar (inserir, atualizar e excluir) informações em um banco de dados.

DDL

Veja linguagem de definição de banco de dados.

deep ensemble

A combinação de vários modelos de aprendizado profundo para gerar previsões. Os deep ensembles podem ser usados para produzir uma previsão mais precisa ou para estimar a incerteza nas previsões.

Aprendizado profundo

Um subcampo do ML que usa várias camadas de redes neurais artificiais para identificar o mapeamento entre os dados de entrada e as variáveis-alvo de interesse.

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

O processo de criar uma aplicação, novos recursos ou correções de código disponíveis no ambiente de destino. A implantação envolve a implementação de mudanças em uma base de código e, em seguida, a criação e execução dessa base de código nos ambientes da aplicação

ambiente de desenvolvimento

Veja ambiente.

controle detectivo

Um controle de segurança projetado para detectar, registrar e alertar após a ocorrência de um evento. Esses controles são uma segunda linha de defesa, alertando você sobre eventos de segurança que contornaram os controles preventivos em vigor. Para obter mais informações, consulte Controles detectivos em Como implementar controles de segurança na AWS.

mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. O DVSM estende o processo de mapeamento do fluxo de valor originalmente projetado para práticas de manufatura enxuta. Ele se concentra nas etapas e equipes necessárias para criar e movimentar valor por meio do processo de desenvolvimento de software.

gêmeo digital

Uma representação virtual de um sistema real, como um prédio, fábrica, equipamento industrial ou linha de produção. Os gêmeos digitais oferecem suporte à manutenção preditiva, ao monitoramento remoto e à otimização da produção.

tabela de dimensões

Em um esquema em estrela, uma tabela menor que contém atributos de dados sobre dados quantitativos em uma tabela de fatos. Os atributos da tabela de dimensões geralmente são campos de texto ou números discretos que se comportam como texto. Esses atributos normalmente são usados para restringir consultas, filtrar e rotular conjuntos de resultados.

desastre

Um evento que impede que uma workload ou sistema cumpra seus objetivos de negócios em seu local principal de implantação. Esses eventos podem ser desastres naturais, falhas técnicas ou o resultado de ações humanas, como configuração incorreta não intencional ou ataque de malware.

Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um disastre. Para obter mais informações, consulte Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework.

DML

Veja linguagem de manipulação de banco de dados.

design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como usar o design orientado por domínio com o padrão strangler fig, consulte Modernizar incrementalmente os serviços web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

DR

Veja recuperação de desastres.

Detecção da oscilação

Rastreamento de desvios de uma configuração de linha de base. Por exemplo, você pode usar AWS CloudFormation para detectar desvios nos recursos do sistema ou AWS Control Tower para detectar mudanças em seu landing zone que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja mapeamento do fluxo de valor de desenvolvimento.

E

EDA

Veja análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada com a computação em nuvem, a computação de borda pode reduzir a latência da comunicação e melhorar o tempo de resposta.

intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte O que é EDI (Intercâmbio eletrônico de dados)?.

criptografia

Um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado.

chave de criptografia

Uma sequência criptográfica de bits aleatórios que é gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva.

endianismo

A ordem na qual os bytes são armazenados na memória do computador. Os sistemas big-endian armazenam o byte mais significativo antes. Os sistemas little-endian armazenam o byte menos significativo antes.

endpoint

Veja endpoint de serviço.

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM).

Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte Criar um serviço de endpoint na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos empresariais (ERP)

Um sistema que automatiza e gerencia os principais processos de negócios (como contabilidade, MES e gerenciamento de projetos) para uma empresa.

criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte Criptografia de envelope na documentação AWS Key Management Service (AWS KMS).

ambiente

Uma instância de uma aplicação em execução. Estes são tipos comuns de ambientes na computação em nuvem:

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um CI/CD pipeline, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de segurança AWS da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS , consulte o guia de implementação do programa.

ERP

Veja planejamento de recursos empresariais.

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões, detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

A tabela central em um esquema em estrela. Ela armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: as que contêm medidas e as que contêm uma chave externa para uma tabela de dimensões.

Antecipar-se à falha

Uma filosofia que usa testes frequentes e incrementais para reduzir o ciclo de vida do desenvolvimento. É uma parte essencial de uma abordagem ágil.

delimitação de isolamento contra falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte AWS Fault Isolation Boundaries.

ramificação de recursos

Veja ramificação.

recursos

Os dados de entrada usados para fazer uma previsão. Por exemplo, em um contexto de manufatura, os recursos podem ser imagens capturadas periodicamente na linha de fabricação.

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como

Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com AWS.

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

prompt few shot

Fornecer a um LLM um pequeno número de exemplos que demonstram a tarefa e o resultado desejado antes de solicitar que ele execute uma tarefa semelhante. Essa técnica é uma aplicação do aprendizado em contexto, em que os modelos aprendem com exemplos (shots) incorporados aos prompts. Prompts few-shot podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também prompts zero-shot.

FGAC

Veja controle de acesso refinado.

Controle de acesso refinado (FGAC)

O uso de várias condições para permitir ou negar uma solicitação de acesso.

migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados via captura de dados de alteração para migrar os dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

FM

Veja modelo de base.

modelo de base (FM)

Uma grande rede neural de aprendizado profundo que vem treinando em grandes conjuntos de dados generalizados e não rotulados. FMs são capazes de realizar uma ampla variedade de tarefas gerais, como entender a linguagem, gerar texto e imagens e conversar em linguagem natural. Para obter mais informações, consulte O que são modelos de base?.

G

IA generativa

Um subconjunto de modelos de IA que foram treinados em grandes quantidades de dados e que podem usar um simples prompt de texto para criar novos artefatos e conteúdo, como imagens, vídeos, texto e áudio. Para obter mais informações, consulte O que é IA generativa?.

bloqueio geográfico

Veja restrições geográficas.

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte Restringir a distribuição geográfica do seu conteúdo na CloudFront documentação.

Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o fluxo de trabalho trunk-based é a abordagem moderna e preferencial.

golden image

Um snapshot de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma golden image pode ser usada para provisionar software em vários dispositivos e ajudar a melhorar a velocidade, a escalabilidade e a produtividade nas operações de fabricação de dispositivos.

estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a restrição da compatibilidade com a infraestrutura existente, também conhecida como brownfield. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais ()OUs. Barreiras de proteção preventivas impõem políticas para

garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja alta disponibilidade.

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas AH são projetados para realizar o failover automático, oferecer consistentemente desempenho de alta qualidade e lidar com diferentes cargas e falhas com impacto mínimo no desempenho.

modernização de historiador

Uma abordagem usada para modernizar e atualizar os sistemas de tecnologia operacional (OT) para melhor atender às necessidades do setor de manufatura. Um historiador é um tipo de banco de dados usado para coletar e armazenar dados de várias fontes em uma fábrica.

dados de hold-out

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de machine learning. Você pode usar dados de hold-out para avaliar a performance do modelo comparando as predições do modelo com os dados de retenção.

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

Dados acessados com frequência, como dados em tempo real ou dados translacionais recentes. Esses dados normalmente exigem uma camada ou classe de armazenamento de alto desempenho para fornecer respostas rápidas às consultas.

hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho normal de DevOps lançamento.

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente, a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

eu

IaC

Veja infraestrutura como código.

Política baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões no Nuvem AWS ambiente.

aplicação ociosa

Uma aplicação que tem um uso médio de CPU e memória entre 5 e 20% em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

IIoT

Veja Internet das Coisas Industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para workloads de produção em vez de atualizar, aplicar patches ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e preditivas do que infraestruturas mutáveis. Para obter mais informações, consulte a prática recomendada Implantar usando infraestrutura imutável no AWS Well-Architected Framework.

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A Arquitetura de Referência de AWS Segurança recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

Um termo que foi introduzido por Klaus Schwab em 2016 para se referir à modernização dos processos de manufatura por meio de avanços em conectividade, dados em tempo real, automação, analytics e IA/ML.

infraestrutura

Todos os recursos e ativos contidos no ambiente de uma aplicação.

Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

Internet industrial das coisas (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações, consulte Criando uma estratégia de transformação digital industrial da Internet das Coisas (IIoT).

VPC de inspeção

Em uma arquitetura de AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS) a Internet e as redes locais. A Arquitetura de Referência de AWS Segurança recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

Internet das coisas (IoT)

A rede de objetos físicos conectados com sensores ou processadores incorporados que se comunicam com outros dispositivos e sistemas pela Internet ou por uma rede de comunicação local. Para obter mais informações, consulte O que é IoT?

interpretabilidade

Uma característica de um modelo de machine learning que descreve o grau em que um ser humano pode entender como as previsões do modelo dependem de suas entradas. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com AWS.

IoT

Veja Internet das Coisas.

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. A ITIL fornece a base para o ITSM.

Gerenciamento de serviços de TI (ITSM)

Atividades associadas a design, implementação, gerenciamento e suporte de serviços de TI para uma organização. Para obter informações sobre a integração de operações em nuvem com ferramentas de ITSM, consulte o guia de integração de operações.

ITIL

Veja biblioteca de informações de TI.

ITSM

Veja gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os dados em si recebem explicitamente um valor de etiqueta de segurança. A interseção entre a etiqueta de segurança do usuário e a etiqueta de segurança dos dados determina quais linhas e colunas podem ser vistas pelo usuário.

zona de pouso

Uma landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

grande modelo de linguagem (LLM)

Um modelo de IA de aprendizado profundo pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder a perguntas, resumir documentos, traduzir texto para outros idiomas e completar frases. Para obter mais informações, consulte O que são LLMs.

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulo.

privilégio mínimo

A prática recomendada de segurança de conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte Aplicar permissões de privilégios mínimos na documentação do IAM.

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também endianness.

LLM

Veja grande modelo de linguagem.

ambientes inferiores

Veja ambiente.

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte Machine learning.

ramificação principal

Veja ramificação.

Malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações sensíveis ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Troia, spyware e keyloggers.

Serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstraídos.

sistema de execução de manufatura (MES)

Um sistema de software para rastrear, monitorar, documentar e controlar processos de produção que convertem matérias-primas em produtos acabados no chão de fábrica.

MAP

Veja Programa de Aceleração da Migração.

mecanismo

Um processo completo em que você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se reforça e se aprimora à medida que opera. Para obter mais informações, consulte Construindo mecanismos no AWS Well-Architected Framework.

conta de membro

Todos, Contas da AWS exceto a conta de gerenciamento, que fazem parte de uma organização em AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

MES

Veja sistema de execução de manufatura.

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

Um protocolo de comunicação leve machine-to-machine (M2M), baseado no padrão de publicação/assinatura, para dispositivos de IoT com recursos limitados.

microsserviço

Um serviço pequeno e independente que se comunica de forma bem definida APIs e normalmente é de propriedade de equipes pequenas e independentes. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte Integração de microsserviços usando serviços sem AWS servidor.

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio

de uma interface bem definida usando leveza. APIs Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte Implementação de microsserviços em. AWS

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da estratégia de migração para a AWS.

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

As informações sobre a aplicação e o servidor necessárias para concluir a migração. Cada padrão de migração exige um conjunto de metadados de migração diferente. Exemplos de metadados de migração incluem a sub-rede, o grupo de segurança e AWS a conta de destino.

padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehospede a migração para o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para migrar para a Nuvem AWS. O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A ferramenta MPA (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de prontidão de uma organização para a nuvem, identificar pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas, usando o CAF. AWS Para mais informações, consulte o guia de preparação para migração. A MRA é a primeira fase da estratégia de migração para a AWS.

estratégia de migração

A abordagem usada para migrar uma workload para a Nuvem AWS. Para obter mais informações, veja a entrada 7 Rs neste glossário e consulte Mobilize sua organização para acelerar migrações em grande escala.

ML

Veja machine learning.

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte Strategy for modernizing applications in the Nuvem AWS.

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Evaluating modernization readiness for applications in the Nuvem AWS.

aplicações monolíticas (monólitos)

Aplicações que são executadas como um único serviço com processos fortemente acoplados. As aplicações monolíticas apresentam várias desvantagens. Se um recurso da aplicação apresentar um aumento na demanda, toda a arquitetura deverá ser escalada. Adicionar ou melhorar os recursos de uma aplicação monolítica também se torna mais complexo quando a base de código cresce. Para resolver esses problemas, é possível criar uma arquitetura de microsserviços. Para obter mais informações, consulte Decompor monólitos em microsserviços.

MPA

Veja Avaliação do Portfólio para Migração.

MQTT

Veja Transporte de Telemetria de Enfileiramento de Mensagens.

classificação multiclasse

Um processo que ajuda a gerar previsões para várias classes (prevendo um ou mais de dois resultados). Por exemplo, um modelo de ML pode perguntar “Este produto é um livro, um carro ou um telefone?” ou “Qual categoria de produtos é mais interessante para este cliente?”

infraestrutura mutável

Um modelo que atualiza e modifica a infraestrutura existente para workloads de produção. Para melhorar a consistência, confiabilidade e previsibilidade, o AWS Well-Architected Framework recomenda o uso de infraestrutura imutável como uma prática recomendada.

O

OAC

Veja controle de acesso de origem.

OAI

Veja identidade de acesso de origem.

OCM

Veja gerenciamento de alterações organizacionais.

migração offline

Um método de migração no qual a workload de origem é desativada durante o processo de migração. Esse método envolve tempo de inatividade prolongado e geralmente é usado para workloads pequenas e não críticas.

OI

Veja integração de operações.

Ola

Veja acordo de nível operacional.

migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

OPC-UA

Veja Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

Um protocolo de comunicação machine-to-machine (M2M) para automação industrial. O OPC-UA fornece um padrão de interoperabilidade com esquemas de criptografia, autenticação e autorização de dados.

acordo de nível operacional (OLA)

Um acordo que esclarece o que os grupos funcionais de TI prometem oferecer uns aos outros para apoiar um acordo de serviço (SLA).

análise de prontidão operacional (ORR)

Uma lista de verificação de perguntas e práticas recomendadas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte Operational Readiness Reviews (ORR) no AWS Well-Architected Framework.

tecnologia operacional (TO)

Sistemas de hardware e software que trabalham com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas de

tecnologia da informação (TI) e tecnologia operacional (TO) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

O processo de modernização das operações na nuvem, que envolve planejamento de preparação, automação e integração. Para obter mais informações, consulte o guia de integração de operações.

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de todos Contas da AWS em uma organização em AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte Criação de uma trilha para uma organização na CloudTrail documentação.

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usa o OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. Os diretores autenticados podem acessar o conteúdo em um bucket do S3 somente por meio de uma distribuição específica. CloudFront Veja também OAC, que fornece um controle de acesso mais granular e aprimorado.

ORR

Veja análise de prontidão operacional.

OT

Veja tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de Referência de AWS Segurança recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

P

limite de permissões

Uma política de gerenciamento do IAM anexada a entidades principais do IAM para definir as permissões máximas que o usuário ou perfil podem ter. Para obter mais informações, consulte Limites de permissões na documentação do IAM.

Informações de identificação pessoal (PII)

Informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo. Exemplos de PII incluem nomes, endereços e informações de contato.

PII

Veja informações de identificação pessoal.

manual

Um conjunto de etapas predefinidas que capturam o trabalho associado às migrações, como a entrega das principais funções operacionais na nuvem. Um manual pode assumir a forma de scripts, runbooks automatizados ou um resumo dos processos ou etapas necessários para operar seu ambiente modernizado.

PLC

Veja controlador lógico programável.

PLM

Veja gerenciamento do ciclo de vida do produto.

política

Um objeto que pode definir permissões (veja política baseada em identidade), especificar condições de acesso (veja polítca baseada em recurso) ou definir as permissões máximas para todas as contas em uma organização no AWS Organizations (veja política de controle de serviços).

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microsserviço com base em padrões de acesso a dados e outros requisitos. Se seus microsserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microsserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades.

avaliação do portfólio

Um processo de descobrir, analisar e priorizar o portfólio de aplicações para planejar a migração. Para obter mais informações, consulte Avaliar a preparação para a migração.

predicado

Uma condição de consulta que retorna `true` ou `false`, normalmente localizada em uma cláusula `WHERE`.

pushdown de predicados

Uma técnica de otimização de consultas de banco de dados que filtra os dados na consulta antes da transferência. Isso reduz a quantidade de dados que devem ser recuperados e processados do banco de dados relacional e melhora a performance das consultas.

controle preventivo

Um controle de segurança projetado para evitar que um evento ocorra. Esses controles são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Para obter mais informações, consulte Controles preventivos em Como implementar controles de segurança na AWS.

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais

informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

Privacidade por design

Uma abordagem em engenharia de sistemas que leva em consideração a privacidade em todo o processo de desenvolvimento.

zonas hospedadas privadas

Um contêiner que contém informações sobre como você deseja que o Amazon Route 53 responda às consultas de DNS para um domínio e seus subdomínios em um ou mais. VPCs Para obter mais informações, consulte Como trabalhar com zonas hospedadas privadas na documentação do Route 53.

controle proativo

Um controle de segurança desenvolvido para evitar a implantação de recursos não conformes. Esses controles verificam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o guia de referência de controles na AWS Control Tower documentação e consulte Controles proativos em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto (PLM)

O gerenciamento de dados e processos de um produto em todo o seu ciclo de vida, desde a concepção, o desenvolvimento e o lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja ambiente.

controlador lógico programável (PLC)

Na manufatura, um computador altamente confiável e adaptável que monitora as máquinas e automatiza os processos de fabricação.

encadeamento de prompts

Uso da saída de um prompt do LLM como entrada para o próximo prompt para gerar respostas melhores. Essa técnica é usada para dividir uma tarefa complexa em subtarefas, ou para refinar ou expandir iterativamente uma resposta preliminar. Isso ajuda a melhorar a precisão e a relevância das respostas de um modelo e permite resultados mais granulares e personalizados.

pseudonimização

O processo de substituir identificadores pessoais em um conjunto de dados por valores de espaço reservado. A pseudonimização pode ajudar a proteger a privacidade pessoal. Os dados pseudonimizados ainda são considerados dados pessoais.

publish/subscribe (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um MES baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal em que outros microsserviços possam assinar. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

Uma série de etapas, como instruções, usadas para acessar os dados em um sistema de banco de dados relacional SQL.

regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

R

Matriz RACI

Veja responsável, aprovador, consultado, informado (RACI).

RAG

Veja geração aumentada via recuperação.

ransomware

Um software mal-intencionado desenvolvido para bloquear o acesso a um sistema ou dados de computador até que um pagamento seja feito.

Matriz RASCI

Veja responsável, aprovador, consultado, informado (RACI).

RCAC

Veja controle de acesso por linha e coluna.

réplica de leitura

Uma cópia de um banco de dados usada somente para leitura. É possível encaminhar consultas para a réplica de leitura e reduzir a carga no banco de dados principal.

Redefinir arquitetura

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

O máximo período de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

O máximo atraso aceitável entre a interrupção e a restauração do serviço.

refatorar

Veja 7 Rs.

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter informações, consulte Specify which Regiões da AWS your account can use.

regressão

Uma técnica de ML que prevê um valor numérico. Por exemplo, para resolver o problema de “Por qual preço esta casa será vendida?” um modelo de ML pode usar um modelo de regressão linear para prever o preço de venda de uma casa com base em fatos conhecidos sobre a casa (por exemplo, a metragem quadrada).

redefinir a hospedagem

Veja 7 Rs.

versão

Em um processo de implantação, o ato de promover mudanças em um ambiente de produção.

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

A capacidade de uma aplicação de resistir ou se recuperar de interrupções. Alta disponibilidade e recuperação de desastres são considerações comuns ao planejar a resiliência na Nuvem AWS. Para obter mais informações, consulte Nuvem AWS Resilience.

política baseada em recurso

Uma política associada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

matriz responsável, accountable, consultada, informada (RACI)

Uma matriz que define as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsabilizável (A), consultado (C) e informado (I). O tipo de suporte (S) é opcional. Se você incluir suporte, a matriz será chamada de matriz RASCI e, se excluir, será chamada de matriz RACI.

controle responsivo

Um controle de segurança desenvolvido para conduzir a remediação de eventos adversos ou desvios em relação à linha de base de segurança. Para obter mais informações, consulte Controles responsivos em Como implementar controles de segurança na AWS.

reter

Veja 7 Rs.

Retirada

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

Uma tecnologia de IA generativa em que um LLM faz referência a uma fonte de dados autorizada que está fora de suas fontes de dados de treinamento antes de gerar uma resposta. Por exemplo, um modelo RAG pode realizar uma pesquisa semântica na base de conhecimento ou nos dados personalizados de uma organização. Para obter mais informações, consulte O que é RAG (geração aumentada via recuperação)?.

alternância

O processo de atualizar periodicamente um segredo para dificultar o acesso de um invasor às credenciais.

controle de acesso por linha e coluna (RCAC)

O uso de expressões SQL básicas e flexíveis que tenham regras de acesso definidas. O RCAC consiste em permissões de linha e máscaras de coluna.

RPO

Veja objetivo de ponto de recuperação.

RTO

Veja objetivo de tempo de recuperação.

runbook

Um conjunto de procedimentos manuais ou automatizados necessários para realizar uma tarefa específica. Eles são normalmente criados para agilizar operações ou procedimentos repetitivos com altas taxas de erro.

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login Console de gerenciamento da AWS ou chamar as operações da AWS API sem que você precise criar um usuário no IAM

para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja política de controle de serviço.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte What's in a Secrets Manager secret? na documentação do Secrets Manager.

segurança desde a concepção

Uma abordagem em engenharia de sistemas que leva em consideração a segurança em todo o processo de desenvolvimento.

controle de segurança

Uma barreira de proteção técnica ou administrativa que impede, detecta ou reduz a capacidade de uma ameaça explorar uma vulnerabilidade de segurança. Existem quatro tipos primários de controles de segurança: preventivos, detectivos, responsivos e proativos.

hardening da segurança

O processo de reduzir a superfície de ataque para torná-la mais resistente a ataques. Isso pode incluir ações como remover recursos que não são mais necessários, implementar a prática recomendada de segurança de conceder privilégios mínimos ou desativar recursos desnecessários em arquivos de configuração.

sistema de gerenciamento de eventos e informações de segurança (SIEM)

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

Uma ação predefinida e programada projetada para responder ou remediar automaticamente um evento de segurança. Essas automações servem como controles de segurança responsivos ou detectivos que ajudam você a implementar as melhores práticas AWS de segurança. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a aplicação de patches em uma instância do Amazon EC2 ou a alternância de credenciais.

Criptografia do lado do servidor

Criptografia dos dados em seu destino, por AWS service (Serviço da AWS) quem os recebe.

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização em AWS Organizations. SCPs defina barreiras ou estabeleça limites nas ações que um administrador pode delegar a usuários ou funções. Você pode usar SCPs como listas de permissão ou listas de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte Políticas de controle de serviço na AWS Organizations documentação.

service endpoint (endpoint de serviço)

O URL do ponto de entrada para um AWS service (Serviço da AWS). Você pode usar o endpoint para se conectar programaticamente ao serviço de destino. Para obter mais informações, consulte Endpoints do AWS service (Serviço da AWS) na Referência geral da AWS.

acordo de serviço (SLA)

Um acordo que esclarece o que uma equipe de TI promete fornecer aos clientes, como tempo de atividade e performance do serviço.

indicador de nível de serviço (SLI)

Uma avaliação de um aspecto de performance de um serviço, como taxa de erro, disponibilidade ou throughput.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme avaliado por um indicador de nível de serviço.

modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade com a qual você compartilha AWS pela segurança e conformidade na nuvem. AWS é responsável pela segurança da nuvem, enquanto você é responsável pela segurança na nuvem. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada.

SIEM

Veja sistema de gerenciamento de eventos e informações de segurança.

ponto único de falha (SPOF)

Uma falha em um único componente crítico de uma aplicação que pode interromper o sistema.

SLA

Veja cacordo de serviço.

SLI

Veja indicador de nível de serviço.

SLO

Veja objetivo de nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Phased approach to modernizing applications in the Nuvem AWS.

SPOF

Veja ponto único de falha.

esquema em estrela

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores para armazenar atributos de dados. Essa estrutura foi projetada para ser usada em um data warehouse ou para fins de inteligência comercial.

padrão strangler fig

Uma abordagem à modernização de sistemas monolíticos que consiste em reescrever e substituir incrementalmente a funcionalidade do sistema até que o sistema herdado possa ser desativado. Esse padrão usa a analogia de uma videira que cresce e se torna uma árvore estabelecida e, eventualmente, supera e substitui sua hospedeira. O padrão foi apresentado por Martin Fowler como forma de gerenciar riscos ao reescrever sistemas monolíticos. Para ver um exemplo de como aplicar esse padrão, consulte Modernizar incrementalmente os serviços Web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

sub-rede

Um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle supervisório e aquisição de dados (SCADA)

Na manufatura, um sistema que usa hardware e software para monitorar ativos físicos e operações de produção.

symmetric encryption (criptografia simétrica)

Um algoritmo de criptografia que usa a mesma chave para criptografar e descriptografar dados.

testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar a performance. Você pode usar o Amazon CloudWatch Synthetics para criar esses testes.

prompt do sistema

Uma técnica para fornecer contexto, instruções ou orientações a um LLM a fim de direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e a estabelecer regras para interações com os usuários.

T

tags

Pares de valores-chave que atuam como metadados para organizar seus recursos. AWS As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos da . Para obter mais informações, consulte Marcar seus recursos do AWS.

variável-alvo

O valor que você está tentando prever no ML supervisionado. Ela também é conhecida como variável de resultado. Por exemplo, em uma configuração de fabricação, a variável-alvo pode ser um defeito do produto.

lista de tarefas

Uma ferramenta usada para monitorar o progresso por meio de um runbook. Uma lista de tarefas contém uma visão geral do runbook e uma lista de tarefas gerais a serem concluídas. Para cada tarefa geral, ela inclui o tempo estimado necessário, o proprietário e o progresso.

ambiente de teste

Veja ambiente.

treinamento

O processo de fornecer dados para que seu modelo de ML aprenda. Os dados de treinamento devem conter a resposta correta. O algoritmo de aprendizado descobre padrões nos dados de treinamento que mapeiam os atributos dos dados de entrada no destino (a resposta que você deseja prever). Ele gera um modelo de ML que captura esses padrões. Você pode usar o modelo de ML para obter previsões de novos dados cujo destino você não conhece.

gateway de trânsito

Um hub de trânsito de rede que você pode usar para interconectar sua rede com VPCs a rede local. Para obter mais informações, consulte O que é um gateway de trânsito na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de

gerenciamento para você. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços na AWS Organizations documentação.

tuning (ajustar)

Alterar aspectos do processo de treinamento para melhorar a precisão do modelo de ML. Por exemplo, você pode treinar o modelo de ML gerando um conjunto de rótulos, adicionando rótulos e repetindo essas etapas várias vezes em configurações diferentes para otimizar o modelo.

equipe de duas pizzas

Uma pequena DevOps equipe que você pode alimentar com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados. Para obter mais informações, consulte o guia Como quantificar a incerteza em sistemas de aprendizado profundo.

tarefas indiferenciadas

Também conhecido como trabalho pesado, trabalho necessário para criar e operar um aplicativo, mas que não fornece valor direto ao usuário final nem oferece vantagem competitiva. Exemplos de tarefas indiferenciadas incluem aquisição, manutenção e planejamento de capacidade.

ambientes superiores

Veja ambiente.

V

aspiração

Uma operação de manutenção de banco de dados que envolve limpeza após atualizações incrementais para recuperar armazenamento e melhorar a performance.

controle de versões

Processos e ferramentas que rastreiam mudanças, como alterações no código-fonte em um repositório.

emparelhamento da VPC

Uma conexão entre duas VPCs que permite rotear o tráfego usando endereços IP privados. Para ter mais informações, consulte O que é emparelhamento de VPC? na documentação da Amazon VPC.

Vulnerabilidade

Uma falha de software ou hardware que compromete a segurança do sistema.

W

cache quente

Um cache de buffer que contém dados atuais e relevantes que são acessados com frequência. A instância do banco de dados pode ler do cache do buffer, o que é mais rápido do que ler da memória principal ou do disco.

dados mornos

Dados acessados raramente. Ao consultar esse tipo de dados, consultas moderadamente lentas geralmente são aceitáveis.

função de janela

Uma função SQL que executa um cálculo em um grupo de linhas que se relacionam de alguma forma com o registro atual. As funções de janela são úteis para processar tarefas, como calcular uma média móvel ou acessar o valor das linhas com base na posição relativa da linha atual.

workload

Uma coleção de códigos e recursos que geram valor empresarial, como uma aplicação voltada para o cliente ou um processo de backend.

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do

projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

WORM

Veja gravação única e várias leituras.

WQF

Veja AWS Workload Qualification Framework.

gravação única e várias leituras (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada imutável.

Z

exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma vulnerabilidade zero-day.

vulnerabilidade de dia zero

Uma falha ou vulnerabilidade não mitigada em um sistema de produção. Os agentes de ameaças podem usar esse tipo de vulnerabilidade para atacar o sistema. Os desenvolvedores frequentemente ficam cientes da vulnerabilidade como resultado do ataque.

prompt zero shot

Fornecer a um LLM instruções para realizar uma tarefa, mas sem exemplos (shots) que possam ajudar a orientá-lo. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt. Veja também prompts few-shot.

aplicação zumbi

Uma aplicação que tem um uso médio de CPU e memória inferior a 5%. Em um projeto de migração, é comum retirar essas aplicações.

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.