



Construindo uma Enterprise Blueprint Factory usando AWS Service Catalog

AWS Orientação prescritiva



AWS Orientação prescritiva: Construindo uma Enterprise Blueprint Factory usando AWS Service Catalog

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Introdução	1
Visão geral dos negócios	1
Visão geral da solução	2
Público-alvo	2
Objetivos	3
Arquitetura	4
Componentes	6
Repositório de produtos	6
Repositório de configuração	6
Arquivo de configuração	7
Config Pipeline	9
Pipeline de liberação	11
Ciclo de vida do blueprint	14
Criação de blueprint	14
Atualização do Blueprint	14
Exclusão do blueprint	15
Configuração	17
Pré-requisitos	17
Práticas recomendadas	18
Crie repositórios	18
Configure a fábrica	19
Excluir a fábrica	27
Usando a fábrica	29
Pré-requisitos	29
Crie um plano	29
Atualizar o plano	32
Excluir blueprint	33
Solução de problemas	34
Recursos relacionados	37
AWS documentação	37
AWS postagens no blog	37
Colaboradores	38
Autoria	38
Analisando	38

Redação técnica	38
Histórico do documento	39
Glossário	40
#	40
A	41
B	44
C	46
D	49
E	54
F	56
G	58
H	59
eu	60
L	63
M	64
O	68
P	71
Q	74
R	74
S	78
T	82
U	83
V	84
W	84
Z	85
.....	lxxxvii

Construindo uma Enterprise Blueprint Factory usando AWS Service Catalog

Amazon Web Services ([colaboradores](#))

Outubro de 2024 ([histórico do documento](#))

Visão geral dos negócios

Muitas empresas enfrentam desafios ao escalar suas cargas de trabalho na nuvem. Esses desafios organizacionais incluem o seguinte:

- Criação de modelos de infraestrutura como código (IaC) que podem ser reutilizados em grande escala para vários Serviços da AWS
- Validando se os modelos de IaC seguem as melhores práticas de segurança
- Reduzir tarefas [indiferenciadas](#) ou repetitivas que podem reduzir significativamente a produtividade do desenvolvedor e estender o tempo de lançamento no mercado
- Estabelecendo consistência para modelos de IaC
- Reduzir a utilização de recursos, especialmente para a equipe de segurança, para evitar revisões manuais repetíveis

A criação de um modelo de IaC que siga as melhores práticas de segurança exige que você estabeleça grades de proteção e controles de segurança. Tradicionalmente, a equipe da plataforma de nuvem ou a equipe de segurança revisavam manualmente o código em cada modelo de IaC. Como alternativa, os desenvolvedores implantariam o modelo IaC em um ambiente de não produção e confiariam nos [controles de detetive](#) para encontrar quaisquer problemas de segurança. Ambas as abordagens exigem ciclos de feedback iterativos, retardam o processo de desenvolvimento e aumentam o esforço de engenharia manual.

Como resultado, muitas empresas desejam agilizar a criação, validação e lançamento de modelos de IaC. Eles também querem um meio de gerenciar e governar esses modelos após o lançamento. Mecanismos adequados de gerenciamento e governança ajudam você a atualizar modelos e garantir que os desenvolvedores tenham acesso às versões mais recentes. Esses mecanismos também ajudam você a supervisionar e auditar o uso de modelos em toda a organização.

Visão geral da solução

Este guia explica a solução Enterprise Blueprint Factory, que ajuda você a simplificar a criação, validação, publicação, distribuição e consumo de modelos de infraestrutura como código (IaC) em toda a organização. Esses modelos de IaC também são chamados de blueprints. Essa solução oferece suporte a arquivos de blueprint que são AWS CloudFormation [modelos](#) ou AWS Cloud Development Kit (AWS CDK) [construções](#).

O Enterprise Blueprint Factory usa uma abordagem orientada por configuração para automatizar o compartilhamento, a publicação e a distribuição de blueprints. Um desenvolvedor adiciona um blueprint a um repositório de produtos e, em seguida, adiciona as informações do blueprint a um arquivo de configuração. Isso inicia automaticamente um pipeline de lançamento de integração contínua e entrega contínua (CI/CD). Esse pipeline valida que o esquema segue as melhores práticas AWS de segurança. Isso ajuda a garantir que os projetos da sua organização sejam protegidos por design. A segurança por design é uma abordagem de engenharia de sistemas que leva a segurança em consideração durante todo o processo de desenvolvimento.

A Enterprise Blueprint Factory lança plantas como produtos em [AWS Service Catalog](#). Ao usar o Service Catalog, os usuários finais podem implantar rapidamente os blueprints aprovados que você fornece. O Service Catalog também foi projetado para fornecer recursos de gerenciamento e governança para que os administradores possam definir [controles de acesso refinados](#) e supervisionar o uso do blueprint.

Público-alvo

A seção de [arquitetura do Enterprise Blueprint Factory](#) ajuda arquitetos, gerentes e líderes técnicos a avaliar essa solução e determinar se ela é adequada para sua organização. Esta seção descreve o que são blueprints, como você pode usar o Service Catalog para gerenciá-los e a arquitetura do Enterprise Blueprint Factory.

A seção [Configurando o Enterprise Blueprint Factory](#) ajuda DevOps os engenheiros a implantar o Enterprise Blueprint Factory em seu AWS ambiente. Ele inclui instruções detalhadas para configurar os repositórios necessários e o pipeline de configuração.

A seção [Usando o Enterprise Blueprint Factory](#) ajuda os desenvolvedores de blueprints a criar, atualizar ou excluir blueprints em seu ambiente. Ele fornece instruções detalhadas para gerenciar um blueprint durante todo o seu ciclo de vida. Para criar esquemas, os desenvolvedores devem entender

como criar modelos de IaC, como CloudFormation modelos. Este guia não inclui informações ou instruções sobre como definir esses esquemas.

Objetivos

O Enterprise Blueprint Factory ajuda sua organização a obter os seguintes benefícios:

- Valide se os esquemas seguem as melhores práticas AWS de segurança
- Automatize e padronize o processo de lançamento e validação de projetos
- Melhore a produtividade do desenvolvedor reduzindo o número de tarefas manuais que eles devem realizar
- Use controles de acesso refinados para determinar quais blueprints os usuários finais podem acessar
- Use o controle de versão para gerenciar as atualizações do blueprint e compartilhá-las com os usuários finais
- Ajude os usuários finais a fazerem o autoatendimento na descoberta e no lançamento de projetos
- Supervisionar e auditar o uso de plantas em toda a organização

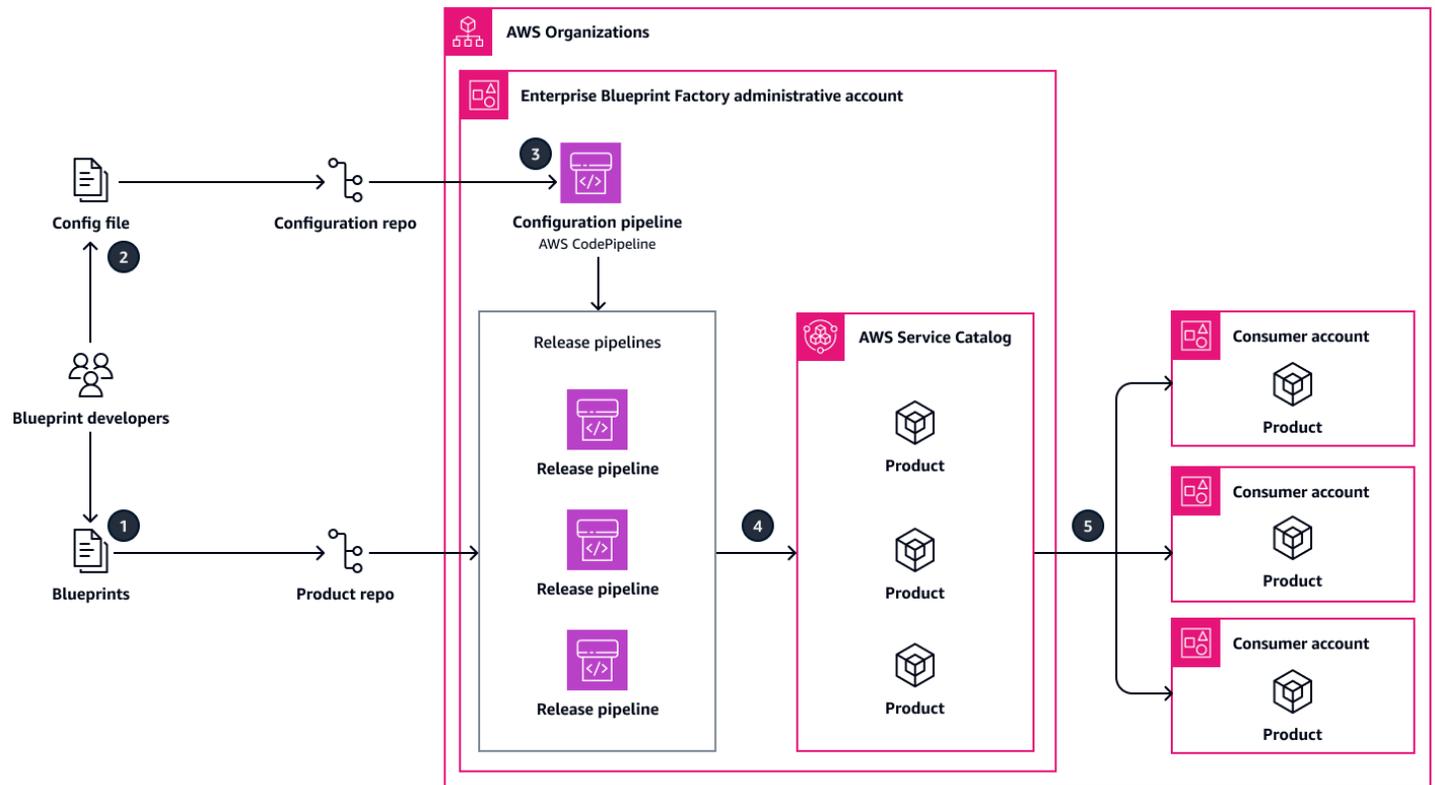
Arquitetura Enterprise Blueprint Factory

Um modelo de infraestrutura como código (IaC), também chamado de blueprint, é um arquivo de configuração que ajuda você a provisionar e gerenciar recursos de nuvem. Um blueprint pode provisionar um único recurso ou pode provisionar a arquitetura para um aplicativo complexo de várias camadas. O IaC foi projetado para ajudá-lo a centralizar o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente.

O Enterprise Blueprint Factory ajuda você a simplificar a criação, validação, publicação, distribuição e consumo de blueprints em toda a sua organização. Além de fornecer uma visão geral da arquitetura, esta seção analisa os [componentes arquitetônicos](#) da solução e o [ciclo de vida do blueprint](#).

[Quando você lança um blueprint por meio do Enterprise Blueprint Factory, o blueprint se torna um produto em. AWS Service Catalog](#) Você coleta produtos em um ou mais [portfólios](#) e, em seguida, concede permissões que permitem que os usuários finais acessem os produtos desse portfólio. Você pode usar um [compartilhamento de portfólio](#) para permitir que um administrador do Service Catalog de outro Conta da AWS distribua seus produtos aos usuários finais.

O diagrama a seguir mostra uma visão geral de alto nível da arquitetura Enterprise Blueprint Factory. Esse fluxo de trabalho libera o blueprint como um produto no Service Catalog. Ele também cria ou atualiza os portfólios e as ações do portfólio para disponibilizar o plano para os usuários-alvo.



Esse diagrama mostra o seguinte fluxo de trabalho:

1. Um desenvolvedor cria o projeto. Eles criam uma ramificação de recursos no repositório do produto, enviam o blueprint para a ramificação e, em seguida, criam uma pull request. Uma equipe administrativa e uma equipe de segurança do blueprint analisam o pull request para garantir que o blueprint atenda aos requisitos organizacionais e de segurança. Essas equipes aprovam o pull request. O desenvolvedor mescla a ramificação de recursos com a ramificação principal. Para obter mais informações, consulte [Repositório de produtos](#) neste guia.
2. O desenvolvedor adiciona ou atualiza as informações do blueprint no arquivo de configuração que está localizado no repositório de configuração. Para obter mais informações, consulte [Repositório de configuração e Arquivo de configuração](#) neste guia.
3. A atualização do arquivo de configuração invoca o pipeline de configuração. Esse pipeline usa [AWS CodePipeline](#) e [AWS CodeBuild](#) para criar ou atualizar os portfólios e os compartilhamentos de portfólio do Service Catalog. Ele também cria um pipeline de lançamento para o projeto. Para obter mais informações, consulte [Pipeline de configuração](#) neste guia.
4. O pipeline de lançamento executa várias verificações de segurança no projeto. Se o blueprint for aprovado, o pipeline de lançamento implantará o blueprint como um produto no Service Catalog. Para obter mais informações, consulte [Release pipeline](#) neste guia.

5. Ao acessar o produto por meio de portfólios e compartilhamentos de portfólio, os usuários finais implantam o plano em suas contas de consumidores-alvo.

Componentes do Enterprise Blueprint Factory

O Enterprise Blueprint Factory consiste nos seguintes componentes:

- [Repositório de produtos](#) — Um repositório onde você armazena os blueprints.
- [Repositório de configuração](#) — Um repositório onde você armazena o arquivo de configuração que define seus AWS Service Catalog portfólios e produtos.
- [Arquivo de configuração](#) — O arquivo de configuração que define quais blueprints estão disponíveis, quem pode usá-los e como eles podem usá-los.
- [Pipeline de configuração](#) — um pipeline de DevOps CI/CD que configura o portfólio e os compartilhamentos do portfólio do Service Catalog e cria um pipeline de lançamento para cada produto.
- Pipeline de [lançamento — um pipeline](#) de DevOps CI/CD que libera blueprints como produtos do Service Catalog.

A equipe de infraestrutura de nuvem normalmente gerencia o Enterprise Blueprint Factory geral porque precisa aprovar cada plano. No entanto, a equipe de DevOps código geralmente é responsável pelo pipeline de configuração e pelo pipeline de lançamento. Para lançar novos esquemas, os desenvolvedores interagem somente com o repositório do produto, o repositório de configuração e o arquivo de configuração.

Repositório de produtos

O repositório de produtos é um local centralizado onde você armazena os planos aprovados pela sua organização. Uma equipe administrativa e uma equipe de segurança do blueprint analisam as pull requests para esse repositório para garantir que cada blueprint atenda aos requisitos organizacionais e de segurança. Neste guia, usamos GitHub para o repositório, mas você pode usar uma alternativa.

Repositório de configuração

O repositório de configuração (repositório de configuração) é o local em que sua organização armazena o arquivo de configuração para seus portfólios e produtos do Service Catalog que são

lançados por meio do Enterprise Blueprint Factory. Neste guia, usamos GitHub para o repositório, mas você pode usar uma alternativa.

Arquivo de configuração

O arquivo de configuração do Enterprise Blueprint Factory (arquivo de configuração) é armazenado no repositório de configuração, que é de propriedade da equipe administrativa do blueprint.

O nome desse arquivo é `bp_config.yml`. Quando um desenvolvedor atualiza esse arquivo, a equipe administrativa do blueprint analisa as alterações. A fusão das alterações na ramificação principal inicia o pipeline de configuração. O arquivo de configuração orquestra a publicação, o compartilhamento e a distribuição de todos os blueprints gerenciados por meio do Enterprise Blueprint Factory.

O arquivo de configuração é um arquivo YAML que consiste em dois objetos principais: `e`. `portfolios` `products` Veja a seguir um exemplo de um exemplo de arquivo de configuração:

```
portfolios:
  - portfolio_name: blueprint-portfolio
    owner: Blueprint-team
    provider_name: AWS
    description: "Blueprint portfolio"
    portfolio_access_role:
      - arn:aws:iam::123456789012:role/examplerole
      - arn:aws:iam::123456789012:user/exampleuser
    share_to_ou:
      - org_id: "o-exampleOrgID"
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
products:
  - name: BP-S3-Product
    description: "Blueprint for BP-S3 product"
    product_config_file: 'BP-S3/product_config.json'
    owner: Blueprint-team
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
    portfolio_associations:
      - blueprint-portfolio
    launch_constraint_role: arn:aws:iam::123456789012:role/examplelaunchrole
```

No `portfolios` objeto, você define seus portfólios de destino do Service Catalog. Para cada portfólio, você fornece os seguintes atributos:

- `portfolio_name` é o nome do portfólio. Esse atributo é obrigatório.
- `owner` é o nome da equipe proprietária do portfólio. Esse atributo é opcional.
- `provider_name` é o nome da equipe ou organização que gerencia o portfólio. O valor padrão é AWS. Esse atributo é obrigatório.
- `description` é uma breve descrição do portfólio. Esse atributo é opcional.
- `portfolio_access_role` são as [identidades AWS Identity and Access Management \(IAM\)](#) (usuários, funções ou grupos) que têm permissão para acessar o portfólio e seus produtos associados. Esse atributo é opcional.
- `share_to_ou` é a [unidade organizacional](#) (OU) na AWS Organizations qual o portfólio é compartilhado. Os usuários finais podem implantar os produtos desse portfólio nos Contas da AWS quais são membros da UO de destino. Esse atributo é opcional.
- `stack_tags` são as [tags](#) aplicadas ao portfólio. Esse atributo é opcional.

No `products` objeto, você define cada blueprint que deseja lançar como um produto no Service Catalog. Para cada produto, você fornece os seguintes atributos:

- `name` é o nome do produto no Service Catalog. Esse atributo é obrigatório.
- `description` é uma breve descrição do produto. Esse atributo é obrigatório.
- `product_config_file` é o nome do arquivo de configuração do produto blueprint que está armazenado no repositório do produto. Esse atributo é obrigatório.
- `owner` é o nome da equipe proprietária do produto. Esse atributo é obrigatório.
- `stack_tags` são as etiquetas aplicadas ao produto. Esse atributo é opcional.
- `portfolio_associations` são os portfólios-alvo que contêm o produto. Esse atributo é opcional.

Note

Recomendamos que você adicione produtos somente aos portfólios gerenciados por meio do Enterprise Blueprint Factory. Se você quiser adicionar produtos aos portfólios que não são gerenciados pelo Enterprise Blueprint Factory, a política de IAM do usuário deve permitir a [AssociateProductWithPortfolio](#) ação. No entanto, como prática recomendada

de segurança, recomendamos que você permita essa ação somente para o pipeline de configuração do Enterprise Blueprint Factory.

- `launch_constraint_role` é a [função de lançamento](#) que o Service Catalog assume quando um usuário final lança o produto. Esse atributo é obrigatório.

Pipeline de configuração

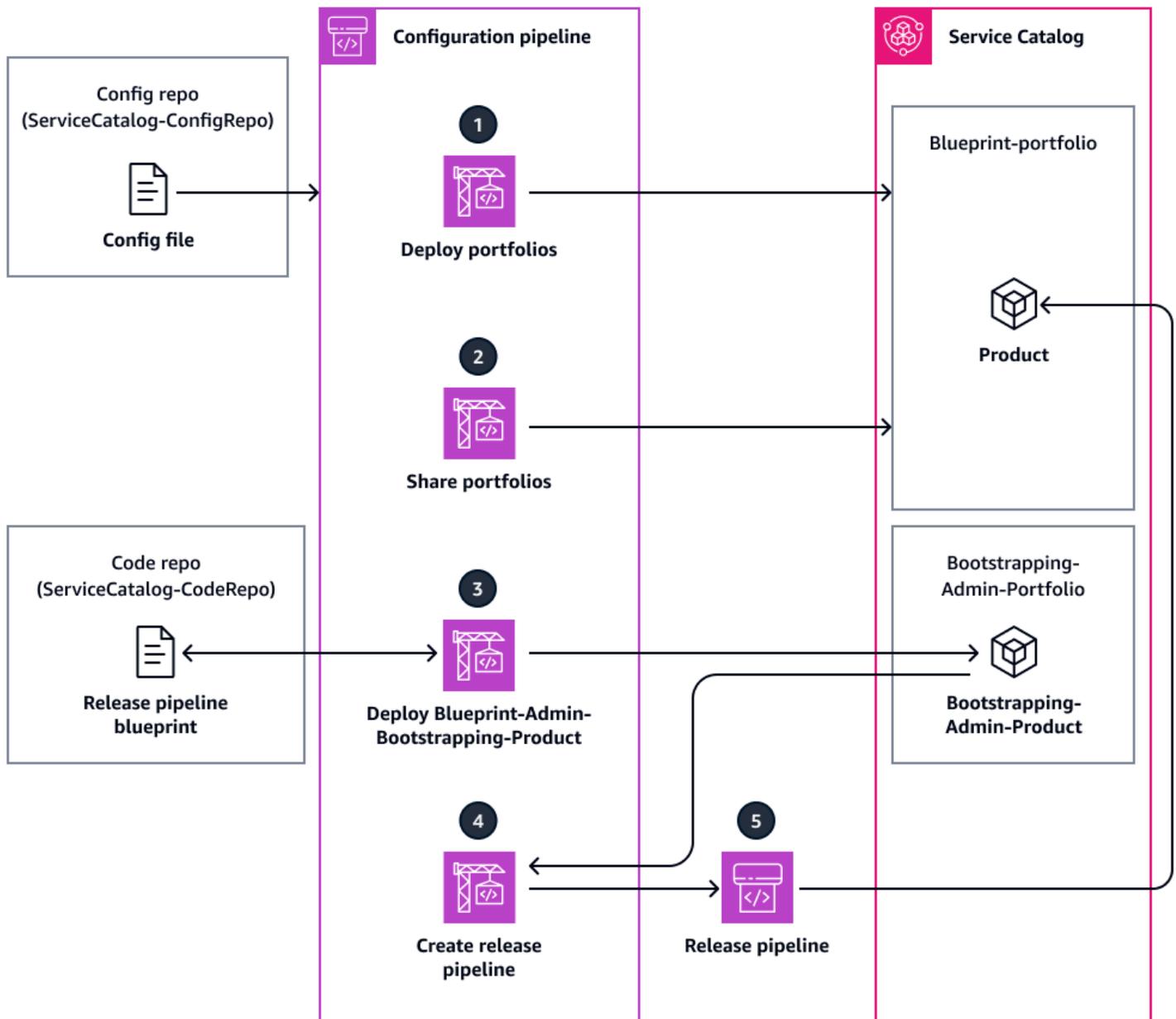
O pipeline de configuração (config pipeline) automatiza a configuração do portfólio e dos compartilhamentos do portfólio do Service Catalog. Ele também cria o pipeline de lançamento para cada produto. Esse pipeline é um [AWS CodePipeline](#) recurso. Uma atualização no arquivo de configuração invoca o pipeline de configuração.

Na primeira vez que você invoca o pipeline de configuração, ele cria dois portfólios adicionais que não estão definidos no seu arquivo de configuração:

- **Blueprint-portfolio**— Cada produto que você implanta por meio do Enterprise Blueprint Factory é adicionado a esse portfólio. Esse portfólio está disponível para os diretores e unidades organizacionais do IAM que você especifica no arquivo de configuração.
- **Bootstrapping-Admin-Portfolio**— O `Bootstrapping-Admin-Product` produto está associado a esse portfólio. Este produto é um CloudFormation modelo para o pipeline de lançamento. Permita que somente a equipe administrativa do blueprint acesse esse portfólio para que ela possa gerenciar produtos administrativos.

Etapas do pipeline de configuração

A imagem a seguir mostra os estágios do pipeline de configuração e os recursos com os quais o pipeline interage. Cada estágio do pipeline é um [AWS CodeBuild](#) projeto.



A seguir estão os estágios do pipeline de configuração:

1. Implantar portfólios — O pipeline de configuração implanta todos os portfólios que foram adicionados ao arquivo de configuração ou exclui todos os portfólios que foram removidos do arquivo de configuração. Se não houver alterações nos portfólios, o pipeline pulará esse estágio.
2. Compartilhe portfólios — O pipeline de configuração compartilha os portfólios com as unidades organizacionais de destino (). OUs Se não houver alterações nas ações do portfólio, o pipeline pulará esse estágio.

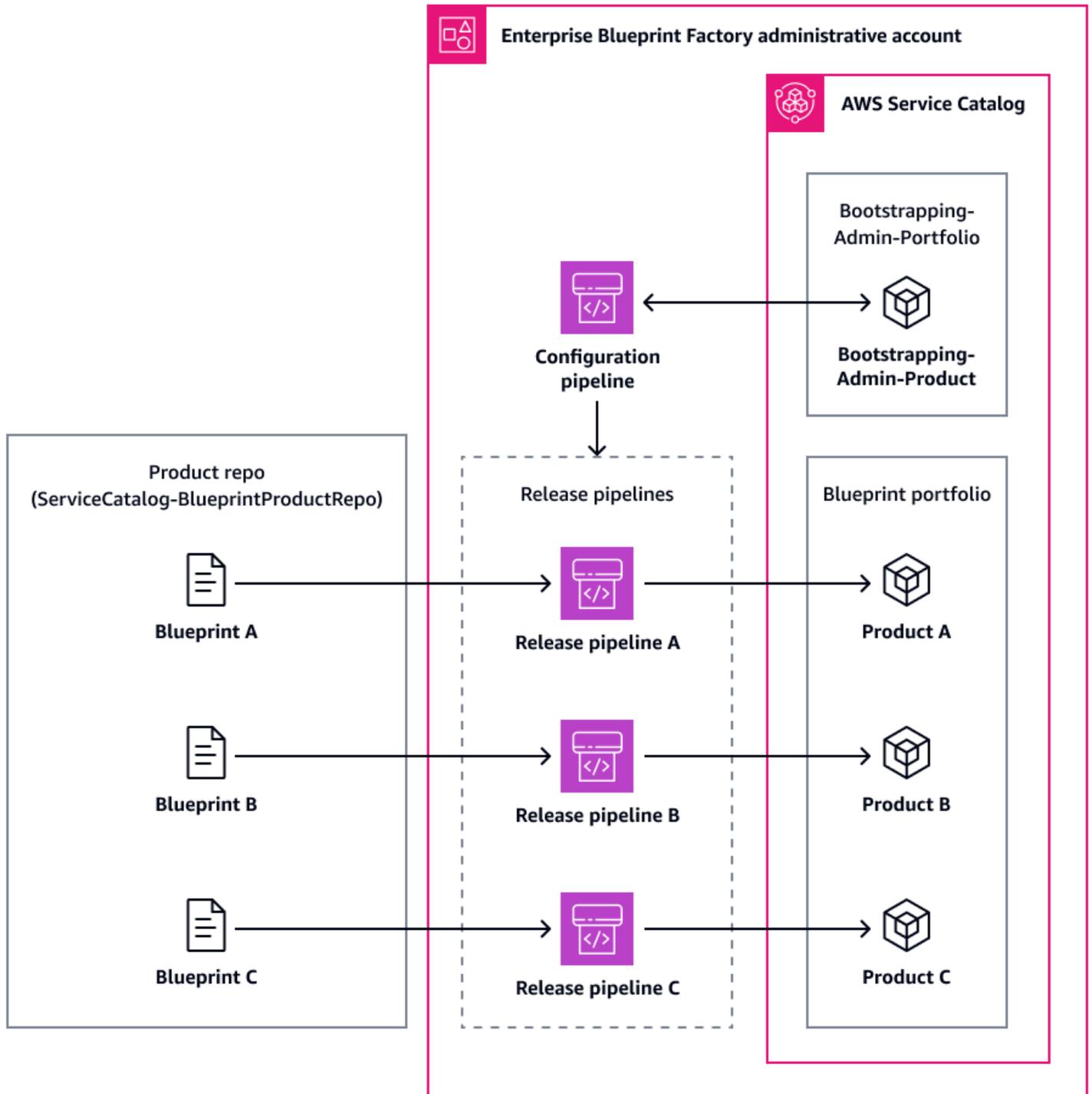
3. Implantar Blueprint-Admin-Bootstrapping-Product — O pipeline de configuração busca o `bp-pipeline` blueprint do `ServiceCatalog-CodeRepo` repositório e o implanta no Service Catalog como `Bootstrapping-Admin-Product`. Esse produto é o CloudFormation modelo usado para criar um pipeline de lançamento. A implantação desse modelo como um produto do Service Catalog ajuda a manter o controle de versão. Se não houver alterações no `bp-pipeline` blueprint, o pipeline pulará esse estágio.
4. Crie pipelines de lançamento — Com base nos atributos do produto no arquivo de configuração, o pipeline de configuração prepara os parâmetros da pilha e inicia uma CloudFormation pilha que cria um pipeline de lançamento para o produto. Para obter mais informações, consulte [Release pipeline](#) neste guia.
5. Implantar produtos — O pipeline de lançamento implanta o blueprint como um produto do Service Catalog e o associa ao portfólio de destino. Agora, os usuários finais podem implantar o produto em Contas da AWS membros da UO de destino.

Pipeline de liberação

O pipeline de lançamento automatiza o lançamento de blueprints como produtos do Service Catalog. Esse pipeline é um [AWS CodePipeline](#) recurso. Quando sua organização deseja lançar um novo blueprint, um desenvolvedor carrega o modelo de IaC e o arquivo de configuração do produto no repositório do produto. Adicionar os detalhes do produto ao arquivo de configuração aciona o pipeline de configuração. O pipeline de configuração cria um pipeline de lançamento para esse blueprint. Qualquer atualização subsequente do blueprint acionará esse pipeline de lançamento para atualizar o produto no Service Catalog com uma nova versão.

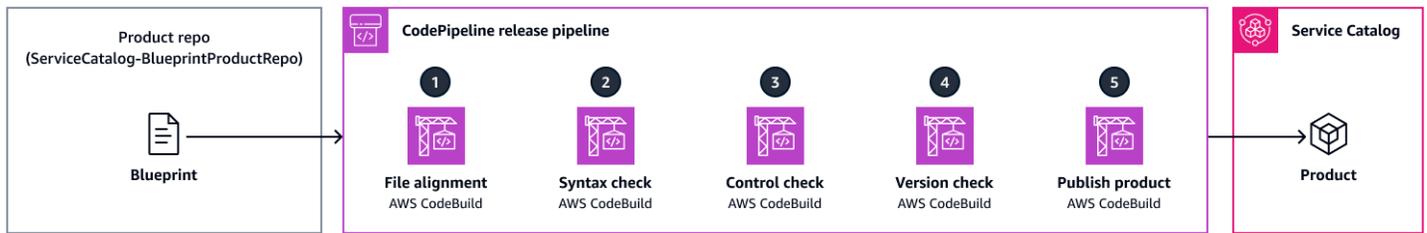
O pipeline de lançamento inclui [controles proativos](#) que automatizam as verificações de segurança e conformidade de seus planos. Os controles proativos são projetados para evitar a criação de recursos não compatíveis. Esses controles podem reduzir o número de eventos de segurança manipulados por outros tipos de controles de [segurança, como controles](#) responsivos e de detetive. Como os controles proativos garantem que os recursos implantados estejam em conformidade antes de serem implantados, não há nenhum evento de detecção que exija resposta ou correção.

Na primeira vez que você invoca o pipeline de configuração, ele cria um produto Service Catalog chamado `Bootstrapping-Admin-Product`. Este produto é o CloudFormation modelo para o pipeline de lançamento. Conforme mostrado na figura a seguir, o pipeline de configuração usa o `Bootstrapping-Admin-Product` produto para criar um pipeline de lançamento dedicado para cada novo blueprint. Existe uma one-to-one relação entre os projetos e os pipelines de lançamento.



Etapas do pipeline de lançamento

A imagem a seguir mostra os estágios padrão no pipeline de lançamento e os recursos com os quais o pipeline interage. Cada estágio do pipeline é um CodeBuild projeto.



A seguir estão os estágios do pipeline de lançamento:

1. Alinhamento do arquivo — [Esse estágio verifica se o blueprint é um CloudFormation modelo ou uma construção. AWS Cloud Development Kit \(AWS CDK\)](#) Se o projeto for uma AWS CDK construção, esse estágio sintetiza a AWS CDK construção em um modelo. CloudFormation Esse processo automatiza e padroniza as implantações por meio de. CloudFormation Se algum erro for encontrado, o pipeline falhará.
2. Verificação de sintaxe — O erro de sintaxe é uma causa comum de erros de CloudFormation implantação. [Nesse estágio, o AWS CloudFormation Linter \(cfn-lint\) verifica erros de sintaxe comparando o modelo com a especificação do recurso.AWS CloudFormation](#) Ele também executa outras verificações, como a verificação de valores válidos para as propriedades dos recursos e a adesão às melhores práticas. Se algum erro for encontrado, o pipeline falhará e o cfn-lint retornará sugestões.
3. Verificação de controle — Neste estágio, [cfn_nag](#) verifica possíveis problemas de segurança pesquisando padrões. Por exemplo, ele verifica grupos de segurança e políticas AWS Identity and Access Management (IAM) excessivamente permissivos, criptografia ausente e literais de senha. Se algum erro for encontrado, o pipeline falhará e cfn_nag retornará sugestões.
4. Verificação de versão — O pipeline de lançamento executa o controle de versão com base na estratégia de versão definida no arquivo de configuração do produto. Se a versão do produto for definida como [imutável](#), o Service Catalog inativará a versão anterior do produto.
5. Publicar produto — O pipeline de lançamento libera o produto no Service Catalog.

Note

O pipeline de lançamento é personalizável. Por exemplo, você pode remover qualquer estágio que não seja aplicável ao seu caso de uso. Você também pode adicionar mais estágios se quiser adicionar outras verificações de controle, validações adicionais ou uma etapa de aprovação manual. Este guia não inclui instruções para modificar o pipeline de

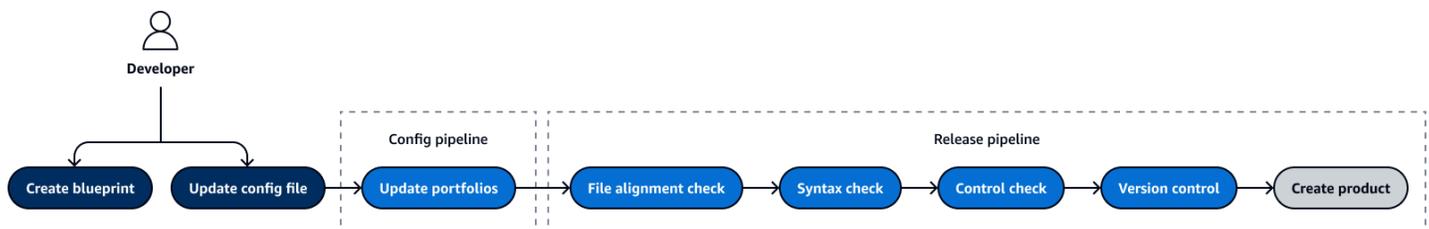
lançamento. Para obter mais informações, consulte [CodePipeline](#) e [CodeBuild](#) documentação e.

Ciclo de vida do Blueprint na Enterprise Blueprint Factory

O ciclo de vida de um blueprint do Enterprise Blueprint Factory consiste em três estágios típicos: criação, atualização e exclusão. O estágio do ciclo de vida afeta as ações que o pipeline de configuração e o pipeline de lançamento executam.

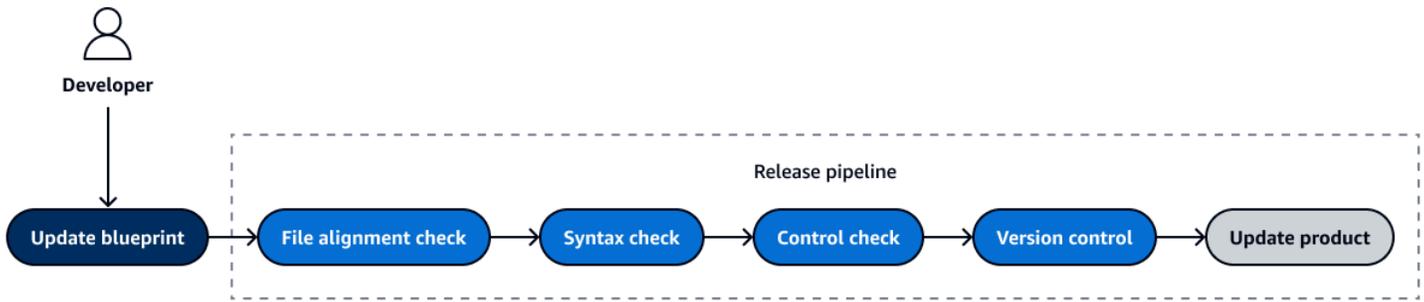
Criação de blueprint

Para lançar um novo blueprint como produto em AWS Service Catalog, um desenvolvedor mescla o blueprint no repositório do produto, atualiza os portfólios no arquivo de configuração e adiciona o novo produto ao arquivo de configuração. Isso invoca o pipeline de configuração. O pipeline de configuração cria um pipeline de lançamento para o produto. No pipeline de lançamento, o projeto passa por várias verificações de segurança. Em seguida, o pipeline de lançamento implanta o blueprint como um produto do Service Catalog.

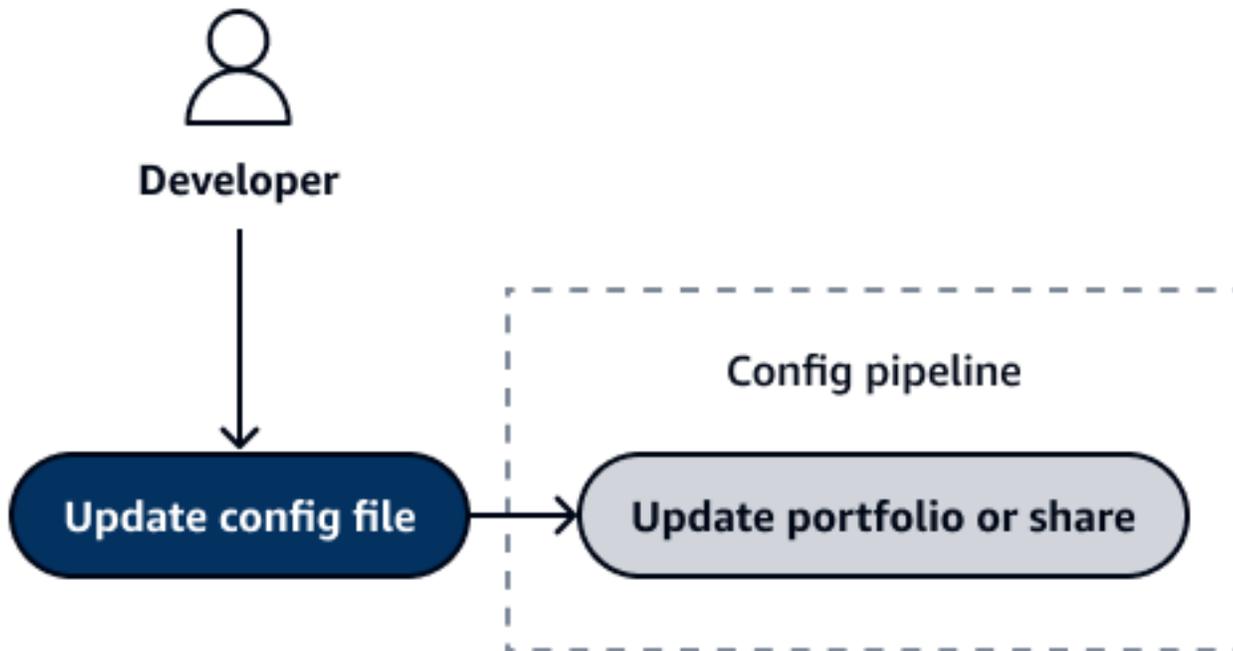


Atualização do Blueprint

Um desenvolvedor pode atualizar o produto no Service Catalog mesclando uma versão atualizada do blueprint no repositório do produto. Essa atualização invoca o pipeline de lançamento do produto. O modelo atualizado passa pelas verificações de segurança no pipeline de lançamento. O pipeline de lançamento implanta uma nova versão do produto Service Catalog. Para obter mais informações sobre como o Service Catalog atualiza a versão do produto, consulte [Gerenciando versões](#) na documentação do Service Catalog.



Como alternativa, você pode atualizar a qual portfólio do Service Catalog o blueprint está associado ou alterar as configurações de compartilhamento desses portfólios. Nesse caso, o desenvolvedor atualiza o arquivo de configuração no repositório de configuração. O pipeline de configuração atualiza os portfólios ou os compartilhamentos do portfólio. Nesse caso, o produto no Service Catalog permanece inalterado, embora agora possa ser incluído em portfólios diferentes.



Exclusão do blueprint

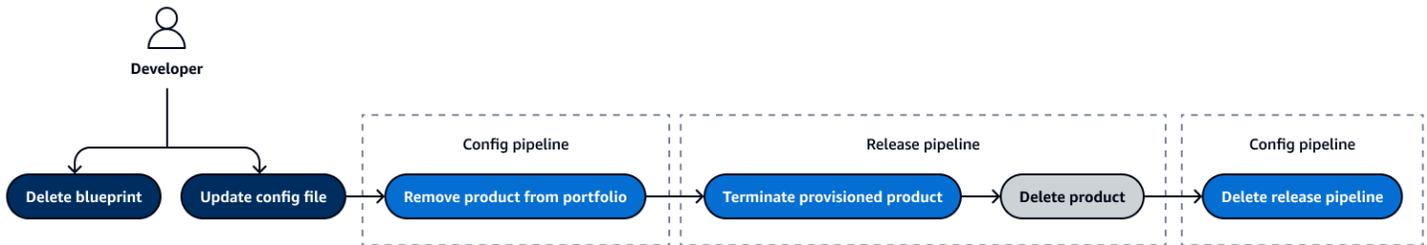
⚠ Important

Você não pode recuperar um produto do Service Catalog depois que ele for excluído. No entanto, você pode reimplantar o blueprint como um novo produto.

Quando você exclui um produto, o Service Catalog remove todas as versões do produto de cada portfólio que contém o produto. Para obter mais informações, consulte [Excluindo produtos](#) na documentação do Service Catalog.

Para excluir um blueprint depois de implantado no Service Catalog, um desenvolvedor exclui o blueprint no repositório do produto. Em seguida, eles removem o produto do arquivo de configuração. O pipeline de configuração dissocia o produto dos portfólios que o contêm e exclui todos os produtos associados. O pipeline de lançamento encerra o produto Service Catalog e os produtos [provisionados](#). Em seguida, o pipeline de configuração exclui o pipeline de lançamento do produto.

Se o pipeline de configuração não conseguir dissociar todos os recursos do produto, o produto não será excluído e o pipeline falhará. Você deve resolver a falha na dissociação de recursos e, em seguida, reiniciar o pipeline. Para obter mais informações, consulte [Resolvendo falhas na dissociação de recursos ao excluir](#) um produto.



Configurando o Enterprise Blueprint Factory

Esta seção ajuda você a configurar o Enterprise Blueprint Factory em seu AWS ambiente. Ele inclui instruções detalhadas para configurar os repositórios e os AWS recursos necessários para o Enterprise Blueprint Factory.

Pré-requisitos

A seguir estão os pré-requisitos para configurar o Enterprise Blueprint Factory em seu ambiente: AWS

- O seguinte Contas da AWS:
 - Uma conta usada para administrar o Enterprise Blueprint Factory e lançar produtos
 - Uma ou mais contas que consomem o produto lançado
- Todas as contas são:
 - Gerenciado como uma organização em [AWS Organizations](#)
 - Localizado na mesma [unidade organizacional \(OU\)](#)
 - A organização segue o [account-per-tenant modelo](#)
- AWS Command Line Interface (AWS CLI), [instalado](#) e [configurado](#)
- Permissões para implantar uma AWS CloudFormation pilha que cria os seguintes AWS recursos:
 - Grupo de CloudWatch registros do Amazon Logs
 - AWS CodePipeline oleodutos
 - AWS CodeBuild projetos
 - Política e regra de ônibus para EventBridge eventos da Amazon
 - AWS Identity and Access Management Papel e política (IAM)
 - AWS Key Management Service (AWS KMS) chave e política chave
 - AWS Service Catalog portfólios, produtos e produtos provisionados
 - Tópico, política de tópicos e assinatura do Amazon Simple Notification Service (Amazon SNS)
 - Buckets do Amazon Simple Storage Service (Amazon S3)
 - AWS Systems Manager Parâmetros do Parameter Store

Para obter mais informações sobre como configurar essas permissões, consulte a [CloudFormation documentação](#) e a [implementação de políticas para permissões de privilégios mínimos](#) para AWS CloudFormation

- Uma GitHub conta

Práticas recomendadas

Recomendamos que você siga estas melhores práticas ao configurar o Enterprise Blueprint Factory em seu AWS ambiente:

- Ao configurar as permissões necessárias para implantar o Enterprise Blueprint Factory, siga o princípio do menor privilégio e conceda as permissões mínimas necessárias. Para obter mais informações, consulte [Concessão de privilégio mínimo](#) e [nas melhores práticas de segurança](#) na documentação do IAM.
- Ao configurar o acesso aos portfólios do Service Catalog, siga o princípio do privilégio mínimo e conceda acesso somente a funções, usuários ou administradores específicos. Siga as [melhores práticas de segurança](#) do Service Catalog.

Criando os repositórios

Esta seção ajuda você a configurar o repositório de [configuração e o repositório](#) de [produtos para o Enterprise Blueprint Factory](#). Para configurar seus repositórios, você [bifurca](#) os repositórios fornecidos em GitHub. Em seguida, você usa Conexões de código da AWS para criar uma [conexão com](#) seu GitHub repositório. Em seguida, você clona os GitHub repositórios na sua máquina local.

Para bifurcar os repositórios GitHub

1. Inicie sessão no [GitHub](#).
2. Navegue até o repositório [do GitHub repositório de configuração](#).
3. Escolha Fork.
4. Na página Criar uma nova bifurcação, na caixa Nome do repositório, digite. ServiceCatalog-ConfigRepo
5. (Opcional) Insira uma descrição.
6. Selecione Copiar somente a ramificação principal.

7. Escolha Criar bifurcação.
8. Repita essas etapas para bifurcar o repositório [Code repo](#) GitHub . Insira o nome ServiceCatalog-CodeRepo desse repositório.
9. Repita essas etapas para bifurcar o repositório do [Product Repo](#) GitHub . Insira o nome ServiceCatalog-BlueprintProductRepo desse repositório.

Para criar a CodeConnections conexão

1. Na AWS CLI, insira o seguinte comando para criar uma CodeConnections conexão com: GitHub

```
aws codeconnections create-connection --provider-type GitHub --connection-name  
<MyConnection>
```

2. Use o console AWS Developer Tools para concluir a conexão. Para obter mais informações, consulte [Atualizar uma conexão pendente](#).

Para clonar os repositórios bifurcados

- Insira os seguintes comandos para clonar os GitHub repositórios em sua estação de trabalho local:

```
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-config-repo  
ServiceCatalog-ConfigRepo  
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-blueprint-repo  
ServiceCatalog-BlueprintProductRepo  
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-code-repo  
ServiceCatalog-CodeRepo
```

Configurando o Enterprise Blueprint Factory

As instruções nesta seção descrevem como configurar o Enterprise Blueprint Factory em sua conta de destino. O repositório de produtos do qual você clonou GitHub contém dois CloudFormation modelos de amostra e BP-S3 BP-SNS Seguindo essas instruções, você implanta esses dois exemplos de blueprints como produtos no Service Catalog.

Para configurar as funções

1. Na conta do desenvolvedor do Blueprint, crie a seguinte política de confiança e salve-a como `sc-enduserrole-trust-policy.json`:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/ServiceCatalogEndUserRole"
    },
    "Action": "sts:AssumeRole"
  }
}
```

2. Insira o comando a seguir para criar a função `ServiceCatalogEndUserRole` do IAM:

```
aws iam create-role \
--role-name ServiceCatalogEndUserRole \
--assume-role-policy-document file:///sc-enduserrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
-- role-name ServiceCatalogEndUserRole
```

Note

Os desenvolvedores usam a `ServiceCatalogEndUserRole` função para provisionar o produto Service Catalog. Essa função não precisa de permissões para criar os recursos definidos no blueprint. Isso segue as melhores práticas de permissões com menos privilégios e segregação de funções.

3. Crie a seguinte política de confiança e salve-a como `sc-launchconstraintrole-trust-policy.json`:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
```

```

    "Service": "servicecatalog.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}
}

```

4. Insira o comando a seguir para criar a função `ServiceCataloglogLaunchConstraintRole` do IAM:

```

aws iam create-role \
--role-name ServiceCataloglogLaunchConstraintRole \
--assume-role-policy-document file://sc-launchconstraintrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCloudFormationFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole

```

5. Adicione a política a seguir à função `ServiceCataloglogLaunchConstraintRole` do IAM. Inclua todas as outras permissões necessárias para os recursos do produto, conforme descrito em [Configurando uma função do Launch](#) na documentação do Service Catalog:

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
        }
      }
    }
  ]
}

```

Note

O Service Catalog usa essa função para implantar a CloudFormation pilha como um produto no Service Catalog. A política de confiança para essa função garante que somente o Service Catalog possa assumi-la. Outros usuários ou serviços não podem assumir essa função. Isso segue a melhor prática de segregação de funções.

6. Crie a seguinte política de confiança e salve-a como `sc-codebuild-trust-policy.json`:

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

7. Insira o comando a seguir para criar a função `codebuild-servicecatalog-admin-role` do IAM:

```
aws iam create-role \
--role-name codebuild-servicecatalog-admin-role \
--assume-role-policy-document file://sc-codebuild-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess \
--role-name codebuild-servicecatalog-admin-role
```

Note

Os CodeBuild trabalhos no pipeline de configuração usam essa função.

Para configurar o bucket do Amazon S3

- Para criar um bucket do Amazon Simple Storage Service (Amazon S3) usado para armazenar CodePipeline os artefatos, siga as instruções [em Criação de um bucket na documentação](#) do Amazon S3. Siga as [melhores práticas de segurança do Amazon S3](#).

Para configurar os AWS Systems Manager parâmetros

- Siga as instruções em [Criando parâmetros do Parameter Store no Systems Manager](#) para criar os parâmetros do Systems Manager na tabela a seguir. Esses parâmetros são usados no CloudFormation modelo que implanta o pipeline de configuração.

Nome do parâmetro	Tipo	Descrição
/blueprints/resources/vpc_id	String	Parâmetro que armazena o ID da nuvem privada virtual (VPC) de destino.
/blueprints/resources/subnets	StringList	Parâmetro que armazena IDs as sub-redes de destino.
/blueprints/resources/securitygroups	StringList	Parâmetro que armazena os grupos IDs de segurança de destino.
/blueprints/resources/artifacts-bucket-name	String	Parâmetro que armazena o nome do bucket do Amazon S3 usado para CodePipeline artefatos.

Nome do parâmetro	Tipo	Descrição
<code>/blueprints/resources/BlueprintRepo</code>	String	Parâmetro que armazena o GitHub repositório em que os blueprints do Enterprise Blueprint Factory são armazenados. O valor padrão é <code><user>/aws-enterprise-blueprint-factory-blueprint-repo</code> .
<code>/blueprints/resources/CodeRepo</code>	String	Parâmetro que armazena o GitHub repositório em que o código do pipeline de configuração do Enterprise Blueprint Factory e o Bootstrapping-Admin-Product código são armazenados. O valor padrão é <code><user>/aws-enterprise-blueprint-factory-code-repo</code> .
<code>/blueprints/resources/ConfigRepo</code>	String	Parâmetro que armazena o GitHub repositório em que os arquivos de configuração do Enterprise Blueprint Factory são armazenados. O valor padrão é <code><user>/aws-enterprise-blueprint-factory-config-repo</code> .

Para atualizar os CloudFormation modelos

1. No repositório de código (ServiceCatalog-CodeRepo), abra o arquivo ServiceCatalog-Pipeline.yml.
2. Edite os valores padrão para os seguintes parâmetros nesse arquivo:
 - `ConfigRepositoryName` é o parâmetro do Systems Manager que armazena o GitHub repositório em que os arquivos de configuração do Enterprise Blueprint Factory são armazenados. O valor padrão é `/blueprints/resources/ConfigRepo`.
 - `CodeRepositoryName` é o parâmetro do Systems Manager que armazena o GitHub repositório em que o código do pipeline de configuração do Enterprise Blueprint Factory e o `Bootstrapping-Admin-Product` código são armazenados. O valor padrão é `/blueprints/resources/CodeRepo`.
 - `BlueprintRepositoryName` é o parâmetro do Systems Manager que armazena o GitHub repositório em que os blueprints do Enterprise Blueprint Factory são armazenados. O valor padrão é `/blueprints/resources/BlueprintRepo`.
 - `BranchName` é a ramificação do repositório de configuração em que o arquivo de configuração é armazenado. O valor padrão é `main`.
 - `VPCID` é o parâmetro do Systems Manager que armazena o ID da VPC de destino. O valor padrão é `/blueprints/resources/vpc_id`.
 - `Subnets` é o parâmetro do Systems Manager que armazena as sub-redes IDs de destino. O valor padrão é `/blueprints/resources/subnets`.
 - `SecurityGroupIds` é o parâmetro do Systems Manager que armazena os grupos IDs de segurança de destino. O valor padrão é `/blueprints/resources/securitygroups`.
 - `IamRoleName` é o nome da função do IAM que os CodeBuild trabalhos usam. O valor padrão é `codebuild-servicecatalog-admin-role`.
 - `EnvironmentType` é o ambiente em que você está implantando o Enterprise Blueprint Factory. O valor padrão é `DEV`.
 - `ArtifactBucket` é o parâmetro do Systems Manager que armazena o bucket do Amazon S3 onde CodePipeline armazena artefatos. O valor padrão é `/blueprints/resources/artifacts-bucket-name`.
 - `CodeConnectionArn` é o Amazon Resource Name (ARN) da CodeConnections conexão a GitHub
3. Salve e feche o arquivo ServiceCatalog-Pipeline.yml.

4. Insira os seguintes comandos para mesclar as alterações no repositório de código:

```
cd ServiceCatalog-CodeRepo
git add ServiceCatalog-Pipeline.yml
git commit -m "<description of change>"
git push origin main
```

5. No repositório de configuração (ServiceCatalog-ConfigRepo), abra o arquivo bp_config.yml.
6. Atualize os valores na seção de portfólio conforme necessário para sua organização. Por exemplo, portfolio_access_roles atualize os share_to_ou atributos e. Para obter mais informações, consulte [Arquivo de configuração](#) neste guia.
7. Salve e feche o arquivo bp_config.yml.
8. Insira os seguintes comandos para mesclar as alterações no repositório de código:

```
cd ServiceCatalog-ConfigRepo
git add bp_config.yml
git commit -m "<description of change>"
git push origin main
```

Para implantar a CloudFormation pilha

1. Faça login na conta administrativa do Enterprise Blueprint Factory.
2. Mude para uma função do IAM que tenha [permissões administrativas](#).
3. Abra o [console de CloudFormation](#).
4. Na barra de navegação na parte superior da tela, escolha o destino Região da AWS.
5. Na página Pilhas, escolha Criar pilha no canto superior direito e selecione Com novos recursos (padrão).
6. Em Prepare template (Preparar modelo), selecione Template is ready (O modelo está pronto).
7. Em Especificar modelo, escolha Fazer upload de um arquivo de modelo.
8. Escolha Escolher arquivo, navegue até a ServiceCatalog-CodeRepo pasta e escolha ServiceCatalog-Pipeline.yml.
9. Escolha Avançar para continuar e validar o modelo.
10. Em Nome da pilha, insira um nome para a pilha.

11. Na seção Parâmetros, não altere os valores padrão.
12. Escolha Próximo.
13. Na página Configurar opções de pilha, não altere os valores padrão e escolha Avançar.
14. Na página Revisar e criar, verifique os detalhes do modelo e da pilha e escolha Enviar.
15. Monitore o progresso da implantação da pilha. Para obter mais informações, consulte a [documentação do CloudFormation](#).
16. Aguarde até que o status mude para CREATE_COMPLETE.

Para validar a implantação

1. Abra o [console de AWS Service Catalog](#).
2. No painel de navegação, escolha Produtos.
3. Confirme se ServiceCatalog-Pipeline está disponível na lista de produtos.
4. Abra o [console de AWS CodePipeline](#).
5. Em Nome, escolha o pipeline de configuração. Por padrão, o nome do pipeline é ServiceCatalog-Pipeline.
6. Selecione Visualizar histórico.
7. Visualize o status da execução do pipeline e do estágio. Para obter mais informações sobre o status, consulte [Exibir status de execução](#) na CodePipeline documentação.
8. Espere até que o status do pipeline de configuração seja Succeeded.
9. Abra o [console do Service Catalog](#).
10. No painel de navegação, escolha Produtos.
11. Confirme se os produtos BP-S3 e BP-SNS estão disponíveis. Isso indica que os pipelines de lançamento do produto para os esquemas de amostra foram concluídos com êxito.
12. Se você quiser excluir os exemplos de blueprints que você implantou ao configurar o Enterprise Blueprint Factory, siga as instruções em [Excluindo](#) um blueprint.

Excluir o Enterprise Blueprint Factory

Se você não estiver usando o Enterprise Blueprint Factory, poderá excluí-lo para parar de incorrer nos custos associados aos seus AWS recursos.

Para excluir os recursos do

1. Insira os seguintes comandos para excluir as funções do IAM que foram implantadas na conta administrativa do Enterprise Blueprint Factory:

```
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \  
--role-name ServiceCatalogEndUserRole  
aws iam delete-role --role-name ServiceCatalogEndUserRole  
aws iam detach-role-policy \  
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \  
--role-name ServiceCataloglogLaunchConstraintRole  
aws iam delete-role --role-name ServiceCataloglogLaunchConstraintRole
```

2. Exclua a CloudFormation pilha da Enterprise Blueprint Factory. Para obter instruções, consulte [Excluir uma pilha do CloudFormation console](#) ou [Excluir uma pilha do AWS CLI](#).
3. Exclua o bucket do Amazon S3 usado para armazenar os CodePipeline artefatos. Para obter instruções, consulte [Excluir um bucket](#) na documentação do Amazon S3.
4. Exclua os seguintes parâmetros do Systems Manager do Parameter Store:
 - /blueprints/resources/vpc_id
 - /blueprints/resources/subnets
 - /blueprints/resources/securitygroups
 - /blueprints/resources/artifacts-bucket-name
 - /blueprints/resources/BlueprintRepo
 - /blueprints/resources/CodeRepo
 - /blueprints/resources/ConfigRepo

Para obter instruções, consulte [Excluindo parâmetros do Parameter Store](#) na documentação do Systems Manager.

Usando o Enterprise Blueprint Factory

Esta seção ajuda você a criar, atualizar ou excluir blueprints em seu ambiente. Ele fornece instruções detalhadas para gerenciar um blueprint durante todo o seu [ciclo de vida](#).

[Para criar ou atualizar esquemas personalizados, você deve ter uma compreensão de como criar modelos de IaC, como AWS CloudFormation modelos ou AWS Cloud Development Kit \(AWS CDK\) construções](#). Este guia não inclui informações ou instruções sobre como definir os blueprints que você lança por meio do Enterprise Blueprint Factory.

Pré-requisitos

A seguir estão os pré-requisitos para usar o Enterprise Blueprint Factory em seu ambiente: AWS

- AWS Command Line Interface (AWS CLI), [instalado](#) e [configurado](#)
- Permissões para assumir a função `ServiceCatalogEndUserRole` AWS Identity and Access Management (IAM)
- Um CloudFormation modelo ou AWS CDK construção

Criação de um plano

Os pipelines do Enterprise Blueprint Factory implantam os blueprints que você define no arquivo de configuração. O desenvolvedor inicia o pipeline de configuração mesclando o arquivo de configuração no repositório de configuração. Em seguida, o Enterprise Blueprint Factory usa o `ServiceCatalogLaunchConstraintRole` para implantar o blueprint como um produto no Service Catalog. Para obter mais informações sobre as ações que o pipeline de configuração e o pipeline de lançamento executam quando você cria um blueprint, consulte [Criação de blueprint](#) neste guia.

Para adicionar o blueprint ao repositório do produto

1. Certifique-se de ter configurado seu Enterprise Blueprint Factory de acordo com as instruções em [Configurando o Enterprise Blueprint Factory](#) neste guia.
2. Confirme se a política da `ServiceCatalogLogLaunchConstraintRole` função permite que você provisione os recursos definidos no blueprint.

3. No repositório do produto (ServiceCatalog-BlueprintProductRepo), crie uma pasta para o novo blueprint.
4. Cole o modelo do IaC (CloudFormation modelo ou AWS CDK construção) na pasta que você criou.
5. Crie um arquivo chamado product_config.json na pasta que você criou.
6. Abra o arquivo product_config.json e cole o seguinte no arquivo:

```
{
  "SchemaVersion": "1.0",
  "ProductVersionName": "1.0.1",
  "Deprecated_Versions" : [],
  "ProductVersionDescription": "<description>",
  "ProductType": "CLOUD_FORMATION_TEMPLATE",
  "Properties": {
    "TemplateFilePath": "./<folder name>/<file name>"
  }
}
```

Em que:

- <description>é uma breve descrição da versão do blueprint
- <folder name>é o nome da pasta que você criou no repositório do produto
- <file name>é o nome do modelo IaC

 Note

Você pode atualizar a versão do esquema ou os nomes das versões do produto de acordo com as políticas da sua organização.

7. Salve e feche o arquivo product_config.json.
8. Insira os seguintes comandos para mesclar as alterações no repositório do produto:

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "The first version of <file name> blueprint"
git push origin main
```

Para atualizar o arquivo de configuração

1. No repositório de configuração (ServiceCatalog-ConfigRepo), abra o arquivo config.yml.
2. Edite a portfolios seção e a products seção conforme necessário para o novo blueprint. Para obter mais informações, consulte [Arquivo de configuração](#) neste guia.
3. Salve e feche o arquivo config.yml.
4. Insira os seguintes comandos para mesclar as alterações no repositório de configuração:

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

A aprovação dessa pull request inicia o pipeline de configuração. O pipeline de configuração cria um pipeline de lançamento para o produto.

Para revisar os registros de implantação

1. Faça login na conta administrativa do Enterprise Blueprint Factory.
2. Abra o [console de AWS CodePipeline](#).
3. Em Nome, escolha o pipeline de lançamento do produto. Por padrão, o nome do pipeline é Blueprint_<Product-Name>-<CloudFormation-Stack-Name>.
4. Selecione Visualizar histórico.
5. Visualize o status da execução do pipeline e do estágio. Para obter mais informações sobre o status, consulte [Exibir status de execução](#) na CodePipeline documentação.
6. Se a tubulação falhar, analise a causa da falha. Para obter instruções sobre como configurar o monitoramento para seus pipelines, consulte [Monitoramento de pipelines](#) na CodePipeline documentação. Se o pipeline de lançamento falhar devido a uma verificação de cfn-lint ou cfn_nag, corrija o erro no modelo. Envie outra pull request para o repositório do produto. Isso reinicia o pipeline de lançamento. Para obter mais informações sobre como corrigir erros de modelo, consulte a seção [Solução de problemas](#) neste guia.
7. Espere até que o status do pipeline de lançamento seja Succeeded.

Para validar a implantação

1. Faça login em uma conta de consumidor na organização.
2. Assuma a função `ServiceCatalogEndUserRole` do IAM.
3. Abra o [console do Service Catalog](#).
4. No painel de navegação, escolha Produtos.
5. Confirme se o novo produto está disponível na lista de produtos.

Atualizar um esquema

Para obter mais informações sobre as ações que o pipeline de configuração e o pipeline de lançamento executam quando você cria um blueprint, consulte [Atualização do blueprint](#) neste guia.

Para atualizar um blueprint

1. No repositório do produto, navegue até a pasta do produto.
2. Cole o modelo atualizado do IaC. Verifique se o nome do arquivo é o mesmo da versão anterior.
3. Abra o arquivo `product_config.json`.
4. Para `ProductVersionName`, atualize o número da versão.
5. Se você quiser evitar que a versão anterior do produto seja implantada futuramente, para `paraDeprecated_Versions`, insira os números da versão anterior em uma lista separada por vírgulas.
6. Insira os seguintes comandos para mesclar as alterações no repositório do produto:

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "Version <number> of <file name> blueprint"
git push origin main
```

A aprovação dessa pull request inicia o pipeline de lançamento do produto.

Para revisar os registros de implantação

1. Faça login na conta administrativa do Enterprise Blueprint Factory.
2. Abra o [console de AWS CodePipeline](#).

3. Em Nome, escolha o pipeline de lançamento. Por padrão, o nome do pipeline é `BluePrint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Selecione Visualizar histórico.
5. Visualize o status da execução do pipeline e do estágio. Para obter mais informações sobre o status, consulte [Exibir status de execução](#) na CodePipeline documentação.
6. Se a tubulação falhar, analise a causa da falha. Para obter instruções sobre como configurar o monitoramento para seus pipelines, consulte [Monitoramento de pipelines](#) na CodePipeline documentação. Se o pipeline de lançamento falhar devido a uma verificação de cfn-lint ou cfn_nag, corrija o erro no modelo. Envie outra pull request para o repositório do produto. Isso reinicia o pipeline de lançamento. Para obter mais informações sobre como corrigir erros de modelo, consulte a seção [Solução de problemas](#) neste guia.
7. Espere até que o status do pipeline de lançamento seja Succeeded.

Para validar a atualização

1. Faça login em uma conta de consumidor na organização.
2. Assuma a função `ServiceCatalogEndUserRole` do IAM.
3. Abra o [console do Service Catalog](#).
4. No painel de navegação, escolha Produtos.
5. Confirme se a nova versão do produto está disponível na lista de produtos.

Excluindo um blueprint

Quando você exclui um produto, o Service Catalog remove todas as versões do produto de cada portfólio que contém o produto. Para obter mais informações, consulte [Excluindo produtos](#) na documentação do Service Catalog. Para obter mais informações sobre as ações que o pipeline de configuração e o pipeline de lançamento executam quando você cria um blueprint, consulte [Exclusão de blueprint neste guia](#).

Para excluir um blueprint

1. No repositório de configuração, abra o arquivo `config.yml`.
2. Edite a seção de produtos, remova ou comente o produto que você deseja excluir.
3. Salve e feche o arquivo `config.yml`.

4. Insira os seguintes comandos para mesclar as alterações no repositório de configuração:

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

A aprovação dessa pull request inicia o pipeline de configuração. O pipeline de configuração exclui o produto e seu pipeline de lançamento.

5. No repositório do produto, exclua a pasta do produto, incluindo seu conteúdo.
6. Insira os seguintes comandos para mesclar as alterações no repositório do produto:

```
cd ServiceCatalog-BlueprintProductRepo
git add .
git commit -m "Delete <file name> blueprint"
git push origin main
```

Para validar a exclusão

1. Faça login em uma conta de consumidor na organização.
2. Assuma a função `ServiceCatalogEndUserRole` do IAM.
3. Abra o [console do Service Catalog](#).
4. No painel de navegação, escolha Produtos.
5. Confirme se o produto excluído não está mais disponível.

Solução de problemas

Quando você cria ou atualiza um blueprint, as ferramentas `cfn-lint` e `cfn-nag` validam o blueprint. Para obter mais informações sobre validação no pipeline de lançamento, consulte [Release pipeline](#) neste guia. Qualquer erro de sintaxe ou segurança relatado faz com que o pipeline falhe. Para implantar com êxito o blueprint por meio do pipeline de lançamento, você deve corrigir os erros no blueprint.

Veja a seguir um exemplo de saída que mostra dois erros relacionados à segurança, uma falha e um aviso.

```
BP-SNS.yml
```

```
-----  
BP-SNS.yml  
-----  
| WARN W47  
|  
| Resource: ["ExampleTopic"]  
| Line numbers: [5]  
|  
| SNS Topic should specify KmsMasterKeyId property  
-----  
| FAIL F18  
|  
| Resource: ["ExampleTopicPolicy"]  
| Line numbers: [10]  
|  
| SNS topic policy should not allow * principal  
  
Failures count: 1  
Warnings count: 1
```

Para corrigir esses erros, no arquivo do blueprint, você substituiria o * principal na política de tópicos do Amazon Simple Notification Service (Amazon SNS) e associaria uma chave AWS Key Management Service (AWS KMS) ao tópico. O exemplo de código a seguir demonstra essas atualizações.

```
ExampleTopic:  
  Type: AWS::SNS::Topic  
  Properties:  
    TopicName: ExampleTopic  
ExampleTopicPolicy:  
  Type: AWS::SNS::TopicPolicy  
  Properties:  
    KmsMasterKeyId: alias/aws/sns # Added KMS key  
    PolicyDocument:  
      Id: Id1  
      Version: '2012-10-17'  
      Statement:  
      - Sid: Sid2  
        Effect: Allow  
        Principal:  
          "Service" : "s3.amazonaws.com" # Replaced "AWS": '*'  
        Action: 'sns:Publish'
```

```
Resource: !Ref ExampleTopic
Topics:
  - !Ref ExampleTopic
```

Recursos relacionados

AWS documentação

- [Tutorial: criar um pipeline que seja implantado no Service Catalog](#) (AWS CodePipeline documentação)
- [AWS CodePipeline documentação](#)
- [AWS CodeBuild documentação](#)
- [Guia do administrador do AWS Service Catalog](#)
- [AWS Service Catalog Guia do usuário](#)

AWS postagens no blog

- [Relate e visualize sua AWS Service Catalog propriedade](#) (postagem AWS no blog)
- [Implementação de um alarme para detectar automaticamente o desvio nas AWS CloudFormation pilhas](#) (AWS postagem do blog)

Colaboradores

As seguintes pessoas contribuíram para este guia.

Autoria

- Haofei Feng, arquiteto sênior de nuvem, AWS
- Cam Maxwell, consultor de segurança principal, AWS
- Joe Guo, engenheiro de suporte de nuvem, AWS
- Shreejesh MV, arquiteto sênior de nuvem, AWS

Analisando

- Joseph Dominic, arquiteto de nuvem, AWS
- Naresh Rajaram, arquiteto de soluções de parceiros de consultoria, AWS

Redação técnica

- Lilly AbouHarb, redatora técnica sênior, AWS

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
Publicação inicial	—	10 de outubro de 2024

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/rearquitar:** 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: migre seu banco de dados Oracle local para a edição compatível com o Amazon Aurora 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: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) for Oracle no. Nuvem AWS
- **Recomprar (drop and shop):** mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a 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: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. 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 local para um serviço em nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para o. AWS
- **Rever (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 atributos](#).

serviços abstratos

Veja os [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 no qual 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.

função agregada

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 a [inteligência artificial](#).

AIOps

Veja as [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 aplicativos

Uma abordagem de segurança que permite o uso somente de aplicativos aprovados 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 descryptografia. É possível compartilhar a chave pública porque ela não é usada na descryptografia, 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 ruim

Um [bot](#) destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o [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 do aplicativo em um ambiente (azul) e a nova versão do aplicativo no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Um aplicativo de software que executa tarefas automatizadas pela Internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como rastreadores da Web que indexam informações na Internet. Alguns outros bots, conhecidos como bots ruins, têm como objetivo perturbar ou causar danos a indivíduos ou organizações.

botnet

Redes de [bots](#) infectadas por [malware](#) e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots 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 em vidro quebrado

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 [Implementar procedimentos de quebra de vidro na orientação do Well-Architected AWS](#) .

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 containerizados 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

Consulte [Estrutura de adoção da AWS nuvem](#).

implantação canária

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substituirá a versão atual em sua totalidade.

CCoE

Veja o [Centro de Excelência em Nuvem](#).

CDC

Veja [a captura de dados de alterações](#).

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 a [integração e a 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 recomendadas 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 CCoE](#) no Blog de Estratégia Nuvem AWS Empresarial.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem geralmente está conectada à tecnologia de [computação de ponta](#).

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 quando migram para o 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

Consulte o [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 GitHub ou 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 da [IA](#) que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Para uma carga de trabalho, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a carga de trabalho 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

Um conjunto 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 is commonly described as a 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.

malha de dados

Uma estrutura arquitetônica 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 que oferece suporte à inteligência comercial, como análises. 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

Consulte a [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 o [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 são comumente 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 [desastre](#). Para obter mais informações, consulte [Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework](#).

DML

Veja a [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 a [recuperação de desastres](#).

detecção de deriva

Rastreando desvios de uma configuração básica. 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 o [mapeamento do fluxo de valor do desenvolvimento](#).

E

EDA

Veja a [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 à [computação em nuvem](#), a computação de ponta 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 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 o [endpoint do 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 corporativos (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 pipeline de CI/CD, 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 o [planejamento de recursos corporativos](#).

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](#). Ele armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

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

limite de isolamento de 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 [Limites de isolamento de AWS falhas](#).

ramificação de recursos

Veja a [filial](#).

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.

solicitação rápida

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 contextual, em que os modelos aprendem com exemplos (fotos) incorporados aos prompts. Solicitações rápidas podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também a solicitação [zero-shot](#).

FGAC

Veja o [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 por meio da [captura de dados alterados](#) para migrar 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 o [modelo da fundação](#).

modelo de fundação (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 básicos](#).

G

IA generativa

Um subconjunto de modelos de [IA](#) que foram treinados em grandes quantidades de dados e que podem usar uma simples solicitação de texto para criar novos conteúdos e artefatos, como imagens, vídeos, texto e áudio. Para obter mais informações, consulte [O que é IA generativa](#).

bloqueio geográfico

Veja as [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 baseado em troncos](#) é a abordagem moderna e preferida.

imagem dourada

Um instantâneo de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma imagem dourada 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 (OU)s. 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, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a [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 retenção

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de aprendizado [de máquina](#). Você pode usar dados de retenção para avaliar o desempenho do modelo comparando as previsões 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 típico de uma DevOps versão.

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

laC

Veja a [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.

IloT

Veja a [Internet das Coisas industrial](#).

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. [Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis](#). Para obter mais informações, consulte as melhores práticas de [implantação usando infraestrutura imutável](#) no Well-Architected AWS 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 fabricação por meio de avanços em conectividade, dados em tempo real, automação, análise 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

Consulte [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

Consulte [a biblioteca de informações](#) de TI.

ITSM

Veja o [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](#).

modelo de linguagem grande (LLM)

Um modelo de [IA](#) de aprendizado profundo que é pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder 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 etiquetas](#).

privilegio 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 [um modelo de linguagem grande](#).

ambientes inferiores

Veja o [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 a [filial](#).

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, 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 abstratos.

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

Consulte [Migration Acceleration Program](#).

mecanismo

Um processo completo no qual 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 o [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 microserviço 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 microserviços 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: rehoste a migração para a Amazon EC2 com o AWS 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 o. 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 carga de trabalho para o. Nuvem AWS Para obter mais informações, consulte a entrada de [7 Rs](#) neste glossário e consulte [Mobilize sua organização para acelerar migrações em grande escala](#).

ML

Veja o [aprendizado de máquina](#).

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 [Estratégia para modernizar aplicativos no 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 [Avaliação da prontidão para modernização de aplicativos no. 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](#).

MAPA

Consulte [Avaliação do portfólio de migração](#).

MQTT

Consulte 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 cargas de trabalho 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 o [controle de acesso de origem](#).

CARVALHO

Veja a [identidade de acesso de origem](#).

OCM

Veja o [gerenciamento de mudanças 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 a [integração de operações](#).

OLA

Veja o [contrato em 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

Consulte [Comunicação de processo aberto — Arquitetura unificada](#).

Comunicação de processo aberto — Arquitetura unificada (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 melhores práticas 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 Well-Architected AWS Framework.

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) 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 todas as 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 a [análise de prontidão operacional](#).

OT

Veja a [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 as [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

Consulte [controlador lógico programável](#).

AMEIXA

Veja o gerenciamento [do ciclo de vida do produto](#).

política

Um objeto que pode definir permissões (consulte a [política baseada em identidade](#)), especificar as condições de acesso (consulte a [política baseada em recursos](#)) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a política de controle de [serviços](#)).

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microserviço com base em padrões de acesso a dados e outros requisitos. Se seus microserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades. Para obter mais informações, consulte [Habilitar a persistência de dados em microserviços](#).

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 WHERE cláusula.

pressão de predicados

Uma técnica de otimização de consulta 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 o desempenho 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 de engenharia de sistema 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](#) projetado para impedir a implantação de recursos não compatíveis. Esses controles examinam 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 o design, desenvolvimento e lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável (PLC)

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

encadeamento imediato

Usando a 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 no qual outros microsserviços possam se inscrever. 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, responsável, consultado, informado \(RACI\)](#).

RAG

Consulte [Geração Aumentada de 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, responsável, consultado, informado \(RACI\)](#).

RCAC

Veja o [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.

rearquiteta

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 mais informações, consulte [Especificar o que Regiões da AWS sua conta pode usar](#).

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 um aplicativo de resistir ou se recuperar de interrupções. [Alta disponibilidade](#) e [recuperação de desastres](#) são considerações comuns ao planejar a resiliência no. Nuvem AWS Para obter mais informações, consulte [Nuvem AWS Resiliência](#).

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](#).

aposentar-se

Veja [7 Rs](#).

Geração Aumentada de Recuperação (RAG)

Uma tecnologia de [IA generativa](#) na qual 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](#).

alternância

O processo de atualizar periodicamente um [segredo](#) para dificultar o acesso das credenciais por um invasor.

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 o [objetivo do ponto de recuperação](#).

RTO

Veja o [objetivo do 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 AWS Management Console 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 a [política de controle de serviços](#).

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele 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 [O que há em um segredo do Secrets Manager?](#) na documentação do Secrets Manager.

segurança por design

Uma abordagem de engenharia de sistemas que leva em conta 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 principais de controles de segurança: preventivos, detectivos, responsivos e proativos.](#)

fortalecimento 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 correção de uma instância EC2 da Amazon ou a rotação 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 medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida 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 [informações de segurança e sistema de gerenciamento de eventos](#).

ponto único de falha (SPOF)

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

SLA

Veja o contrato [de nível de serviço](#).

ESGUIO

Veja o indicador [de nível de serviço](#).

SLO

Veja o objetivo do [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 [Abordagem em fases para modernizar aplicativos no](#). Nuvem AWS

CUSPE

Veja [um único ponto de falha](#).

esquema de estrelas

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 uso 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 de supervisão 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 o desempenho. Você pode usar o [Amazon CloudWatch Synthetics](#) para criar esses testes.

prompt do sistema

Uma técnica para fornecer contexto, instruções ou diretrizes a um [LLM](#) para direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e 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. 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 o [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 o [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 back-end.

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.

MINHOCA

Veja [escrever uma vez, ler muitas](#).

WQF

Consulte [Estrutura de qualificação AWS da carga de trabalho](#).

escreva uma vez, leia muitas (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, geralmente malware, que tira proveito de uma vulnerabilidade de [dia zero](#).

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.

aviso zero-shot

Fornecer a um [LLM](#) instruções para realizar uma tarefa, mas sem exemplos (fotos) que possam ajudar a orientá-la. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A

eficácia da solicitação zero depende da complexidade da tarefa e da qualidade da solicitação. Veja também a solicitação [de algumas fotos](#).

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.