



AWS Estrutura de adoção da nuvem: perspectiva da plataforma

AWS Orientação prescritiva



AWS Orientação prescritiva: AWS Estrutura de adoção da nuvem: perspectiva da plataforma

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

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

Table of Contents

Bem-vindo	1
Introdução	2
Arquitetura de plataforma	5
Iniciar	5
Definir uma estratégia de várias contas	5
Definir controles preventivos	5
Definir a estrutura da unidade organizacional	6
Definir conectividade de rede	6
Definir a estratégia de DNS	7
Definir padrões de marcação	7
Definir uma estratégia de observabilidade	8
Avançado	8
Definir controles proativos e de detecção	8
Definir padrões para integração de serviços	8
Definir padrões e princípios	8
Excel	9
Definir padrões de remediação	9
Comunicar e refinar políticas	9
Compreender os recursos de gerenciamento financeiro	9
Engenharia de plataforma	11
Início	12
Criar uma zona de pouso e implantar barreiras de proteção	12
Estabelecer autenticação	12
Planejar sua rede	12
Colete, agregue e proteja dados de eventos e logs	13
Estabelecer controles	13
Implementar o gerenciamento financeiro da nuvem	13
Avançado	13
Criar automação da infraestrutura	13
Fornecer serviços centralizados de observabilidade	14
Implementar o gerenciamento de sistemas e a governança da AMI	14
Gerenciar o uso de credenciais	15
Estabelecer ferramentas de segurança	15
Excel	15

Criar e distribuir criações de identidade com automação	15
Adicionar detecção e alertas para padrões anômalos nos ambientes	15
Analisar e modelar ameaças	16
Coletar, revisar e refinar as permissões continuamente	16
Selecione, avalie e melhore continuamente as métricas da sua plataforma	16
Arquitetura de dados	17
Iniciar	17
Definir recurso abrangente	17
Organizar zonas de dados	18
Planejar a agilidade e a democratização dos dados	18
Definir a entrega segura de dados	18
Planejar a economia	18
Avançado	19
Noções básicas sobre engenharia de atributos	19
Planejar para desnormalizar conjuntos de dados	19
Portabilidade e escalabilidade do projeto	20
Excel	20
Projetar um framework configurável	20
Planejar criar um mecanismo analítico unificado	20
Definir DataOps	21
Engenharia de dados	22
Iniciar	22
Implantar um data lake	22
Desenvolver padrões de ingestão de dados	22
Acelerar o processamento de dados	24
Fornecer serviços de visualização de dados	24
Avançado	25
Implementar processamento de dados quase em tempo real	25
Validar a qualidade dos dados	25
Comprovação de serviços de transformação de dados	25
Habilitar a democratização de dados	26
Excel	26
Fornecer orquestração baseada em UI	26
Integrar o DataOps	27
Provisionamento e orquestração	29
Início	29

Implantar um modelo hub-and-spoke de catálogo	29
Criar modelos para reutilização	29
Aplicar parâmetros padrão para reutilização	30
Estabelecer um processo de aprovação	30
Avançado	30
Criar um portal de autoatendimento	30
Habilitar um marketplace privado	31
Gerenciar os direitos	31
Excel	31
Integrar com sistemas de compras	31
Integrar com suas ferramentas de ITSM	31
Implemente um sistema de gerenciamento do ciclo de vida e de distribuição de versões	32
Desenvolvimento de aplicações modernas	33
Iniciar	33
Analisar abordagens modernas	33
Adotar recursos de computação nativos da nuvem	34
Usar containerização	34
Usar bancos de dados modernos	34
Avançado	35
Otimizar sua arquitetura moderna	35
Usar tecnologias de malha de serviços	36
Garantir visibilidade e rastreabilidade	36
Excel	36
Adotar microsserviços	36
Integração e entrega contínuas	38
Iniciar	38
Adotar o gerenciamento de componentes de software	38
Criar os pipelines de CI/CD.	38
Implementar testes automatizados	39
Criar documentação	39
Usar infraestrutura como código	40
Manter e acompanhar métricas padrão	40
Avançado	41
Usar gerenciamento de configuração	41
Integrar monitoramento e registro em log	41
Criar uma cadência para mesclagem	41

Capturar o comportamento pós-implantação	42
Excel	42
Integrar tecnologias de IA/ML	43
Adotar práticas de engenharia do caos	43
Otimizar a performance	44
Implementar a observabilidade avançada	44
Implementar práticas de GitOps	45
Conclusão	46
Outras fontes de leitura	47
Colaboradores	48
Histórico do documento	49
Glossário	50
#	50
A	51
B	54
C	56
D	59
E	63
F	65
G	67
H	68
eu	70
L	72
M	73
O	78
P	80
Q	83
R	84
S	87
T	91
U	92
V	93
W	93
Z	94
.....	xcvi

AWS Cloud Adoption Framework: perspectiva da plataforma

Amazon Web Services ([colaboradores](#))

Outubro de 2023 ([histórico do documento](#))

A transformação digital é o maior fator que permite que os executivos melhorem a experiência, a inovação e a flexibilidade do cliente. Ela usa machine learning (ML), inteligência artificial, big data e a velocidade e a escala da nuvem para atender às mudanças nas condições de negócios e às crescentes necessidades dos clientes.

A [Amazon Web Services \(AWS\)](#) é a plataforma de nuvem mais abrangente e amplamente adotada do mundo. Ela pode ajudar você a transformar sua organização e, ao mesmo tempo, a reduzir os riscos comerciais, melhorar o desempenho ambiental, social e de governança (ESG), aumentar a receita e melhorar a eficiência operacional.

O [AWS Cloud Adoption Framework \(AWS CAF\)](#) usa as práticas recomendadas da AWS para ajudar você a acelerar seus resultados comerciais. Use o AWS (CAF) para identificar e priorizar oportunidades de transformação, avaliar e melhorar sua prontidão para a nuvem e desenvolver iterativamente seu roteiro de transformação.

O AWS CAF agrupa sua orientação em seis perspectivas: Negócios, Pessoas, Governança, Plataforma, Segurança e Operações. Cada perspectiva é abordada em um guia separado. Este guia aborda a perspectiva Plataforma, que se concentra em acelerar a entrega de suas workloads na nuvem com um ambiente de nuvem híbrida escalável e de nível empresarial.

Introdução

Milhões de clientes, incluindo as startups de maior crescimento, as maiores empresas e as principais organizações governamentais, usam a AWS. (Veja [histórias de sucesso de clientes](#) no site da AWS.) Eles podem [migrar e modernizar](#) workloads legadas, tornar-se mais [orientados por dados](#), [automatizar e otimizar](#) processos de negócios e reinventar modelos operacionais. Eles são capazes de melhorar seus [resultados de negócios](#) reduzindo os riscos comerciais, melhorando o desempenho ambiental, social e de governança (ESG), aumentando a receita e melhorando a eficiência operacional.

A capacidade organizacional de usar a nuvem de forma eficaz para se [transformar digitalmente](#) (prontidão organizacional para a nuvem) é reforçada por um conjunto de [recursos fundamentais](#). Uma capacidade é a possibilidade organizacional de usar processos para implantar recursos (pessoas, tecnologia e outros ativos tangíveis ou intangíveis) para alcançar um determinado resultado. O AWS CAF identifica essas capacidades e fornece orientação prescritiva que milhares de organizações em todo o mundo têm usado com sucesso para melhorar sua prontidão para a nuvem e acelerar suas jornadas de transformação digital na nuvem.

O AWS CAF agrupa suas capacidades em seis perspectivas:

- [Business](#)
- [Pessoas](#)
- [Governança](#)
- [Plataforma](#)
- [Segurança](#)
- [Operações](#)

A perspectiva Plataforma se concentra em acelerar a entrega de suas workloads na nuvem com um ambiente de nuvem híbrida escalável e de nível empresarial. Esse ambiente compreende sete recursos mostrados no diagrama a seguir. Esses recursos são gerenciados pelas partes interessadas que estão funcionalmente relacionadas em sua [jornada de transformação da nuvem](#). As partes interessadas usuais incluem o diretor de tecnologia (CTO), líderes de tecnologia, arquitetos e engenheiros.

AWS CAF Platform Perspective Capabilities

Platform Architecture

Establish guidelines, principles, patterns, and guardrails for your cloud environment

Data Engineering

Automate and orchestrate data flows throughout your organization

Data Architecture

Design and evolve a fit-for-purpose analytics and data architecture

Provisioning and Orchestration

Create, manage, and distribute catalogs of approved cloud products to end users

Continuous Integration and Delivery

Rapidly evolve and improve applications and services

Platform Engineering

Build a compliant cloud environment with enhanced security features and packaged, reusable products

Modern Application Development

Build well-architected cloud-native applications

Esses recursos são analisados em detalhes nas seções a seguir deste guia. Cada seção fornece diretrizes sobre como começar, avançar e, finalmente, se destacar em uma capacidade específica.

- [Arquitetura de plataforma](#)
- [Engenharia de plataforma](#)
- [Arquitetura de dados](#)

- [Engenharia de dados](#)
- [Provisionamento e orquestração](#)
- [Desenvolvimento de aplicações modernas](#)
- [Integração e entrega contínuas \(CI/CD\)](#)

A perspectiva Plataforma é uma peça fundamental do AWS CAF. É onexo no qual as decisões tomadas em todas as outras perspectivas convergem para fornecer agilidade e valor aos negócios. As decisões tomadas aqui ajudam ou prejudicam seus objetivos de negócios em um nível fundamental. A perspectiva Plataforma do AWS CAF facilita a criação de um ambiente de nuvem escalável e de nível corporativo que sustenta a transformação da sua organização. Por meio dessa perspectiva, o AWS CAF orienta você no estabelecimento de uma plataforma robusta que pode possibilitar sua jornada para a nuvem, levando a uma transformação e crescimento significativos dos negócios.

Ao trabalhar com a perspectiva Plataforma, leve em consideração as conexões multifuncionais com líderes de negócios que precisam ser desenvolvidas e o valor que elas agregam às suas equipes e organização. Concentre-se ainda mais nas mudanças do modelo operacional e nas topologias da equipe para garantir que os requisitos sejam atendidos. Além disso, procure desenvolver as habilidades de que suas equipes precisam para criar a plataforma e permitir seu uso em todas as equipes de aplicações. Tenha em mente as pessoas, os negócios, a governança, a segurança e os objetivos operacionais de sua organização ao tomar essas decisões, pois elas são fundamentais para garantir a adoção da plataforma e o sucesso de seus esforços.

A AWS e a [Rede de Parceiros da AWS](#) fornecem ferramentas e serviços, como workshops e treinamentos, que podem ajudar você nessa jornada para implementar e melhorar sua postura de segurança. O [AWS Professional Services](#) é uma equipe global de especialistas que pode ajudar você a alcançar resultados específicos relacionados à sua transformação na nuvem por meio de uma coleção de ofertas alinhadas ao AWS CAF.

Arquitetura de plataforma

Estabeleça e mantenha diretrizes, princípios, padrões e barreiras de proteção para seu ambiente de nuvem.

Um [ambiente de nuvem bem arquitetado](#) ajuda você a acelerar a implementação, a reduzir riscos e a impulsionar a adoção da nuvem. O recurso de arquitetura da plataforma cria consenso em sua organização sobre os padrões corporativos que impulsionam a adoção da nuvem. Você define esquemas e barreiras de proteção de práticas recomendadas para facilitar a autenticação, a segurança, a rede, o registro em log e o monitoramento. Além disso, você leva em consideração e planeja as workloads que talvez precise reter on-premises devido aos requisitos de latência, processamento de dados ou residência de dados, e avalia casos de uso da nuvem híbrida, como expansão da nuvem, backup e recuperação de desastres na nuvem, processamento distribuído de dados e computação de borda.

Iniciar

Definir uma estratégia de várias contas

Uma boa [estratégia de várias contas](#) considera questões de escala e eficiência operacional. Isso significa [isolar suas workloads](#) em um padrão lógico que melhor atenda às suas necessidades operacionais. Sugerimos que você comece com um conjunto básico de contas para acomodar serviços centralizados e descentralizados em sua empresa. Você pode centralizar as funções de segurança, financeiras e operacionais para gerenciar e governar com eficácia suas equipes e contas distribuídas e autônomas. Você vai querer se alinhar com toda a sua organização para entender como a plataforma e suas workloads serão segmentadas e gerenciadas. A compreensão dessa estrutura ajuda a garantir que os princípios de segurança estejam em vigor para autenticação e autorização, ao mesmo tempo em que se alinham às políticas de uso aceitável em evolução da plataforma.

Definir controles preventivos

Planeje um ambiente seguro com várias contas com um conjunto incorporado de controles padrão (barreiras de proteção). Comece a entender e a usar um mecanismo como [políticas de controle de serviços \(SCPs\)](#) para gerenciar o uso de serviços em toda a sua organização, incluindo as Regiões da AWS que estão disponíveis para consumo em sua plataforma de nuvem. As políticas fornecem

um mecanismo centralizado para controlar o máximo de permissões disponíveis para todas as contas e garantir que elas sigam as diretrizes de controle de acesso da organização.

Definir a estrutura da unidade organizacional

As unidades organizacionais (UOs) servem como uma forma prática de gerenciar e categorizar contas com base em requisitos regulatórios e ambientes de ciclo de vida de desenvolvimento de software (SDLC). Ao usar UOs, as organizações simplificam o processo de solicitação de políticas e permissões apropriadas em toda a infraestrutura de nuvem. As [UOs de workloads](#) são projetadas especificamente para contas que oferecem suporte a recursos de infraestrutura de aplicações e garantem que as políticas corretas sejam aplicadas. O uso de UOs e SCPs ajuda a aprimorar a segurança e a conformidade da infraestrutura de nuvem da sua organização, além de garantir a operação tranquila de suas aplicações e serviços. Em última análise, isso leva a um processo de adoção da nuvem mais eficiente e robusto.

Definir conectividade de rede

A [conectividade de rede](#) é um aspecto crucial de qualquer infraestrutura de nuvem que ofereça suporte à criação de redes seguras, escaláveis e altamente disponíveis para ser compatível com aplicações e workloads. Uma rede bem projetada fornece alta performance consistente e garante operações contínuas em diferentes ambientes.

Ao projetar sua arquitetura de rede, considere se você tem workloads que deseja manter [on-premises](#) devido aos requisitos de latência, processamento de dados ou residência de dados. Ao avaliar [casos de uso](#) da nuvem híbrida, como expansão na nuvem, backup e recuperação de desastres na nuvem, processamento distribuído de dados e computação de borda, você pode identificar os principais requisitos para os seguintes aspectos:

- Conectividade com e da internet. Esse aspecto envolve o fornecimento de conexões seguras e confiáveis entre suas aplicações ou workloads e a internet. Essa conectividade é essencial para facilitar o acesso a recursos baseados na web, permitir a comunicação entre usuários e aplicações e garantir que seus serviços sejam acessíveis ao público quando necessário.
- Conectividade em seus ambientes de nuvem. Essa área se concentra em estabelecer conexões robustas entre vários componentes e serviços em sua infraestrutura de nuvem. Ela garante que os dados e os recursos sejam facilmente compartilhados e acessados em diferentes serviços em nuvem, promovendo uma colaboração eficiente e operações mais fáceis. Uma consideração importante aqui é o uso de [nuvens privadas virtuais \(VPCs\)](#). Para simplificar as coisas, considere criar padrões sobre como as VPCs são criadas e monitoradas. Considere criar esses padrões

de forma programática e planeje usar uma solução de [gerenciamento de endereços IP \(IPAM\)](#). Aloque espaço IP suficiente para permitir o crescimento e projete estruturas de sub-rede para facilitar a solução de problemas ao usar várias zonas de disponibilidade. Certifique-se de seguir as [práticas recomendadas de segurança para VPCs](#) ao projetar e implementar a conectividade de rede.

- Conectividade entre a rede on-premises e os ambientes de nuvem. Esse aspecto trata da integração de sua infraestrutura on-premises com seu ambiente baseado em nuvem. Ao criar conexões seguras e confiáveis entre os dois, as organizações se beneficiam das vantagens das arquiteturas híbridas. Por exemplo, você pode usar recursos on-premises e serviços em nuvem simultaneamente para melhorar a performance, a escalabilidade e a otimização de custos.

Ao abordar essas três áreas principais de conectividade de rede, você pode criar uma infraestrutura de nuvem robusta que seja compatível com suas aplicações e workloads de forma eficaz, para que você possa aproveitar os benefícios da adoção da nuvem. Anote os requisitos de rede e crie um design simples que permita que você escale de acordo com sua estratégia de várias contas.

Definir a estratégia de DNS

Uma estratégia de DNS bem planejada ajuda a evitar complicações à medida que seus ambientes de nuvem crescem. Se você mantiver recursos de DNS on-premises, recomendamos que você crie [arquiteturas de DNS híbridas](#) que usem a infraestrutura de DNS on-premises junto com o DNS na nuvem para quaisquer requisitos de DNS baseados na nuvem. Integre a resolução de DNS com ambientes DNS on-premises usando endpoints de resolução e regras de encaminhamento. Use zonas hospedadas privadas para armazenar informações sobre como você quer que o DNS da nuvem responda a consultas para um domínio e seus subdomínios dentro de uma ou mais redes.

Definir padrões de marcação

A marcação de recursos é uma prática essencial para gerenciar custos de forma eficaz e identificar a propriedade dos recursos. Considere como sua organização permitirá ainda mais o consumo na nuvem, incluindo o uso de serviços específicos dentro da plataforma. Defina uma estratégia de marcação que rastreie quais recursos estão sendo implantados por quais equipes. Obtenha informações da [perspectiva de operações do AWS CAF](#) e use tags para automatizar tarefas em sua infraestrutura implantada.

Além disso, ao marcar recursos com metadados relevantes, você pode agrupar e monitorar seus gastos com base nos requisitos organizacionais ditados no recurso de gerenciamento financeiro da nuvem (CFM) na [perspectiva de governança do AWS CAF](#). Identifique um mecanismo de geração

de relatórios que apoie suas práticas contábeis e financeiras, incluindo medidas a serem tomadas quando as políticas financeiras forem violadas.

Definir uma estratégia de observabilidade

Estabelecer uma estratégia de observabilidade é uma etapa fundamental para otimizar e proteger sua arquitetura de nuvem. Essa estratégia gira em torno da transformação das métricas e logs produzidos por seus serviços em nuvem em insights acionáveis para a tomada de decisões estratégicas. Priorize o monitoramento dos principais indicadores de performance e a configuração de alertas para abordar preventivamente possíveis problemas. Para evitar a proliferação de ferramentas, otimizar custos e focar o que é mais importante para sua organização, incorpore essa estratégia de observabilidade em sua plataforma e aplicações. Para obter mais orientações, consulte nossa apresentação [Developing an observability strategy](#) (AWS re:Invent 2022).

Avançado

Definir controles proativos e de detecção

Para avançar, sua organização deve identificar a necessidade de controles proativos e de detecção (barreiras de proteção) no ambiente. Crie políticas que definam as barreiras de proteção ou os limites que os perfis e os usuários têm nas contas localizadas em uma unidade organizacional (UO). Analise todas as barreiras de proteção padrão de detecção da plataforma e escolha quais aplicar. Crie controles preventivos e de detecção adicionais, conforme necessário, e agrupe-os por UOs para alinhá-los à sua estratégia de várias contas. Considere de quais ferramentas e mecanismos organizacionais você precisa para inspecionar recursos não compatíveis identificados pelos controles de detecção.

Definir padrões para integração de serviços

Crie padrões para o uso aceitável da plataforma e os padrões associados ao consumo de serviços e como isso será governado. Considere quais serviços iniciais podem ser usados. Crie um documento que descreva esses padrões e publique-os para usuários e operadores da plataforma. Garanta que esses padrões se adaptem ao longo do tempo para atender às mudanças nos objetivos da organização e às capacidades em evolução da computação em nuvem.

Definir padrões e princípios

Considere quais padrões de arquitetura serão permitidos em sua organização usando as informações dos proprietários de aplicações e comece a definir esquemas para a padronização. A

padronização permite maior governança e menor carga administrativa à medida que você escala na nuvem. Defina padrões que usarão a infraestrutura como código (IaC) e planeje um modelo de implantação simplificado usando um catálogo de serviços integrado aos seus processos de controle de mudanças e sistemas de gerenciamento de serviços de TI (ITSM). Defina como esses esquemas serão usados e as circunstâncias para permitir exceções. Planeje essas exceções e sua governança, com considerações sobre autenticação, monitoramento de segurança e proteções.

Excel

Definir padrões de remediação

Considere como anotar e priorizar suas descobertas de barreiras de proteção de detecção para que elas possam ser remediadas de acordo com suas estruturas de segurança e conformidade. Planeje usar a automação para detectar o provisionamento de recursos fora da política, incluindo aqueles que violam as políticas orçamentárias e de marcação. Identifique os recursos necessários para definir e medir os objetivos de serviço enquanto atualiza seus runbooks e playbooks. Defina revisões periódicas dessas práticas e um mecanismo de feedback para capturar dados relacionados à evolução da plataforma. Defina mecanismos para criar e atualizar runbooks e playbooks de forma apropriada.

Comunicar e refinar políticas

Crie um sistema centralizado de gerenciamento de conteúdo para toda a documentação e distribua-o aos usuários e operadores da plataforma. Crie um mecanismo para coletar feedback para futuras considerações sobre mudanças na política.

Compreender os recursos de gerenciamento financeiro

As organizações prosperam quando mantêm uma compreensão transparente e abrangente de seu orçamento. Isso as capacita a tomar decisões bem informadas, alocar recursos com eficiência e atingir seus objetivos estratégicos. Uma visão clara do orçamento ajuda as organizações a se destacar, facilitando a tomada de decisões informadas, a alocação efetiva de recursos, o controle de custos, a avaliação de desempenho e a manutenção da responsabilidade e da conformidade. Em última análise, isso resulta em uma organização mais eficiente, financeiramente estável e próspera. Quando você tem uma estratégia de marcação bem-sucedida, pode usar filtros de custo no [AWS Budgets](#) para filtrar despesas com base nas tags de recursos. Isso ajuda você a criar um orçamento personalizado para projetos, departamentos, ambientes ou outros critérios específicos, aprimorando

ainda mais os recursos de gerenciamento financeiro. Você pode associar as [tags de alocação de custos](#) e as [Categorias de Custos da AWS](#) a tags para gerar insights financeiros e transparência ao relatar custos.

Engenharia de plataforma

Crie um ambiente de nuvem de várias contas seguro e compatível com produtos de nuvem empacotados e reutilizáveis.

Para apoiar a inovação capacitando as equipes de desenvolvimento, a plataforma precisa se adaptar em um ritmo rápido para acompanhar as demandas da empresa. (Consulte a [perspectiva de negócio do AWS CAF](#).) Ela deve fazer isso sendo flexível o suficiente para se adaptar às demandas de gerenciamento de produtos, rígida o suficiente para aderir às restrições de segurança e rápida o suficiente para atender às necessidades operacionais. Esse processo requer a criação de um ambiente de nuvem compatível com várias contas, com recursos de segurança aprimorados e produtos de nuvem empacotados e reutilizáveis.

Um ambiente de nuvem eficaz permite que suas equipes provisionem facilmente novas contas, garantindo que essas contas estejam em conformidade com as políticas organizacionais. Um conjunto selecionado de produtos de nuvem permite que você codifique as práticas recomendadas, ajuda na governança e ajuda a aumentar a velocidade e a consistência de suas implantações na nuvem. Implemente seus esquemas de práticas recomendadas e [barreiras de proteção](#) preventivas e de detecção. [Integre](#) seu ambiente de nuvem com seu cenário existente para viabilizar os casos de uso de nuvem híbrida desejados.

Automatize o fluxo de trabalho de provisionamento de contas e use [várias contas](#) para apoiar suas metas de segurança e governança. Configure a conectividade entre seus ambientes on-premises e na nuvem, bem como entre diferentes contas na nuvem. Implemente a [federação](#) entre seu provedor de identidades (IdP) existente e seu ambiente de nuvem para que os usuários possam se autenticar usando suas credenciais de login existentes. Centralize o registro em log, estabeleça auditorias de segurança entre contas, crie resolvedores de DNS de entrada e saída e obtenha visibilidade de suas contas e barreiras de proteção no painel.

Avalie e certifique os serviços em nuvem para consumo em alinhamento com os padrões corporativos e o gerenciamento de configurações. Empacote e melhore continuamente os padrões corporativos como produtos implantáveis de autoatendimento e serviços consumíveis. Aproveite a [infraestrutura como código \(IaC\)](#) para definir configurações de forma declarativa. Crie equipes de capacitação para evangelizar a plataforma para desenvolvedores e usuários corporativos e permitir que eles criem integrações que acelerem a adoção em toda a organização.

A conclusão das tarefas analisadas nas seções a seguir exige que você crie [recursos](#) e equipes para desenvolver suas organizações em direção à engenharia de plataforma moderna. Para obter detalhes técnicos, consulte o whitepaper [Establishing your Cloud Foundation on AWS](#).

Início

Criar uma zona de pouso e implantar barreiras de proteção

Ao iniciar sua jornada rumo à engenharia de plataforma madura, você deve primeiro implantar sua [zona de pouso](#) com barreiras de proteção preventivas e de detecção, conforme definido no recurso de arquitetura da plataforma. As barreiras de proteção garantem que os padrões organizacionais não sejam violados à medida que os proprietários de aplicações consomem recursos de nuvem. Com esse mecanismo, você automatiza o fluxo de trabalho de provisionamento de contas para usar [várias contas](#) que satisfaçam suas metas de [segurança](#) e [governança](#).

Estabelecer autenticação

Implemente o [gerenciamento de identidade e controle de acesso](#) em todos os ambientes, sistemas, workloads e processos de acordo com os padrões ditados na [perspectiva de segurança do AWS CAF](#). Para identidades da força de trabalho, restrinja o uso de usuários do [AWS Identity and Access Management \(IAM\)](#) e conte com um provedor de identidades que permita gerenciar identidades em um local centralizado. Isso facilita o gerenciamento do acesso em várias aplicações e sistemas, pois você está criando, gerenciando e revogando o acesso de um único local. Use os processos existentes para gerenciar a criação, atualização e remoção do acesso para incluir seus ambientes da AWS .

Planejar sua rede

De acordo com seus projetos de [arquitetura de plataforma](#), crie uma [conta de rede centralizada](#) para controlar o tráfego de entrada e saída de e para seu ambiente. Recomendamos que você projete suas redes para uma conectividade provisionada rapidamente entre sua rede local e seus AWS ambientes, de e para a Internet e entre seus ambientes. AWS A centralização do gerenciamento de rede permite que você implante controles de rede para isolar redes e a conectividade em todo o ambiente usando controles preventivos e reativos.

Colete, agregue e proteja dados de eventos e logs

Use a [observabilidade CloudWatch entre contas da Amazon](#). Ela fornece uma interface unificada para pesquisar, visualizar e analisar métricas, logs e rastreamentos em contas vinculadas, além de eliminar barreiras entre as contas.

Se sua organização tiver requisitos de conformidade específicos para controle e segurança centralizados de logs, considere configurar uma [conta de arquivamento de logs](#) dedicada. Isso oferece um repositório centralizado e criptografado especificamente para dados de logs. Aumente a segurança desse arquivamento alternando regularmente as chaves de criptografia.

Implemente políticas robustas para proteger dados de logs confidenciais, usando [técnicas de mascaramento](#), conforme necessário. Use a agregação de logs para logs de conformidade, segurança e auditoria e garanta o uso de barreiras de proteção rígidas e criações de identidade para evitar alterações não autorizadas nas configurações de logs.

Estabelecer controles

De acordo com as definições da [perspectiva de segurança do AWS CAF](#), implante [recursos básicos de segurança](#) que atendam aos requisitos de seus negócios. Implemente controles [preventivos](#) e de [detecção](#) adicionais, e provisione-os de forma programática e consistente em todas as suas contas, quando necessário. Integre os controles de detecção às ferramentas operacionais, conforme definido pelo recurso de arquitetura da plataforma, para que os recursos não compatíveis possam ser revisados por mecanismos operacionais.

Implementar o gerenciamento financeiro da nuvem

De acordo com a [perspectiva de governança da AWS CAF](#), implemente etiquetas de alocação de AWS custos e Cost Categories que alinhem a estratégia de etiquetagem da sua organização com a responsabilidade financeira pelo consumo da nuvem. AWS As categorias de custos permitem cobrar ou mostrar cobranças de nuvem aos centros de custo internos usando ferramentas como dados [AWS Cost Explorer](#) de faturamento publicados em [AWS Cost and Usage Report](#).

Avançado

Criar automação da infraestrutura

Antes de continuar, avalie e certifique os serviços em nuvem para consumo de acordo com a [arquitetura da sua plataforma](#). Em seguida, empacote e melhore continuamente os padrões

corporativos como produtos implantáveis e serviços consumíveis, e use a infraestrutura como código (IaC) para definir configurações de forma declarativa. A automação da infraestrutura imita os ciclos de desenvolvimento de software ao permitir o acesso a serviços específicos em cada conta com controle de acesso por perfil (RBAC) ou controle de acesso por atributo (ABAC). Implemente um método para provisionar rapidamente novas contas e alinhá-las aos seus recursos de gerenciamento de serviços e incidentes usando APIs ou desenvolvendo recursos de autoatendimento. Automatize a integração da rede e a alocação de IP à medida que as contas são criadas para garantir a conformidade e a segurança da rede. Integre novas contas à sua solução de gerenciamento de serviços de TI (ITSM) usando conectores nativos configurados para operar com a AWS. Atualize seus playbooks e runbooks, conforme apropriado.

Fornecer serviços centralizados de observabilidade

Para obter uma [observabilidade eficaz na nuvem](#), sua plataforma deve oferecer suporte à pesquisa e análise em tempo real de dados de logs locais e centralizados. À medida que suas operações escalam, a capacidade de sua plataforma de indexar, visualizar e interpretar logs, métricas e rastreamentos é fundamental para transformar dados brutos em insights acionáveis.

Ao correlacionar logs, métricas e rastreamentos, você pode extrair conclusões práticas e desenvolver respostas direcionadas e informadas. Estabeleça regras que permitam respostas proativas a eventos ou padrões de segurança identificados em seus logs, métricas ou rastreamentos. À medida que suas AWS soluções se expandem, garanta que sua estratégia de monitoramento seja dimensionada em conjunto para manter e aprimorar seus recursos de observabilidade.

Implementar o gerenciamento de sistemas e a governança da AMI

Organizações que usam instâncias do Amazon Elastic Compute Cloud (Amazon EC2) exigem extensivamente ferramentas operacionais para gerenciar instâncias em grande escala. Gerenciamento de ativos de software, detecção e resposta de endpoints, gerenciamento de inventário, gerenciamento de vulnerabilidades e gerenciamento de acesso são recursos fundamentais para muitas organizações. Esses recursos geralmente são fornecidos por meio de agentes de software instalados nas instâncias. Desenvolva a capacidade de empacotar agentes e outras configurações personalizadas nas imagens de máquina da Amazon (AMIs) e disponibilizá-las para os consumidores da plataforma em nuvem. Use controles preventivos e de detecção que governem o uso dessas AMIs. As AMIs devem conter ferramentas que permitam o gerenciamento de instâncias EC2 de longa execução em grande escala, especialmente para cargas de trabalho mutáveis do Amazon EC2 que não consomem novas regularmente. AMIs Você pode usar o [AWS](#)

[Systems Manager](#) em grande escala para automatizar atualizações de agentes, coletar inventário do sistema, acessar instâncias do EC2 remotamente e corrigir vulnerabilidades do sistema operacional.

Gerenciar o uso de credenciais

De acordo com a [perspectiva de segurança do AWS CAF](#), implemente perfis e credenciais temporários. Use ferramentas para gerenciar o acesso remoto a instâncias ou sistemas on-premises usando um agente pré-instalado sem armazenar segredos. Reduza a dependência de credenciais de longo prazo e verifique se há credenciais codificadas em seus modelos de IaC. Se você não puder usar credenciais temporárias, use ferramentas programáticas, como tokens de aplicações e senhas de banco de dados, para automatizar a alternância e o gerenciamento de credenciais. Codifique usuários, grupos e perfis usando princípios de privilégio mínimo com o IaC e evite a criação manual de contas de identidade usando barreiras de proteção.

Estabelecer ferramentas de segurança

As ferramentas de monitoramento de segurança devem oferecer suporte ao monitoramento granular da segurança em toda a infraestrutura, aplicações e workloads e fornecer visualizações agregadas para análise de padrões. Como acontece com todas as outras ferramentas de gerenciamento de segurança, você deve estender suas ferramentas de detecção e resposta estendidas (XDR) para fornecer funções para avaliar, detectar, responder e remediar a segurança de seus aplicativos, recursos e ambientes de acordo com os requisitos definidos AWS na perspectiva de segurança da [AWS CAF](#).

Excel

Criar e distribuir criações de identidade com automação

Codifique e crie versões de criações de identidade, como perfis, políticas e modelos, com ferramentas de IaC. Use ferramentas de validação de política para verificar avisos de segurança, erros, avisos gerais, alterações sugeridas nas políticas do IAM e outras descobertas. Quando apropriado, implante e remova criações de identidade que forneçam acesso temporário ao ambiente de forma automatizada e proíbam a implantação por indivíduos que estejam usando o console.

Adicionar detecção e alertas para padrões anômalos nos ambientes

Avalie proativamente os ambientes em busca de vulnerabilidades conhecidas e inclua a detecção de padrões incomuns de eventos e atividades. Analise as descobertas e faça recomendações às equipes de arquitetura da plataforma para mudanças que impulsionem mais eficiência e inovação.

Analisar e modelar ameaças

Implemente monitoramento e medição contínuos em relação às avaliações comparativas de segurança e do setor, de acordo com os requisitos sob a [perspectiva de segurança do AWS CAF](#). Ao implementar sua abordagem de instrumentação, determine quais tipos de dados e informações de eventos melhor informarão suas funções de gerenciamento de segurança. Esse monitoramento abrange vários vetores de ataque, incluindo o uso do serviço. Suas bases de segurança devem incluir uma capacidade abrangente de registro em log e analytics seguros em seus ambientes de várias contas, incluindo a capacidade de correlacionar eventos de várias fontes. Evite alterações nessa configuração com controles e barreiras de proteção específicos.

Coletar, revisar e refinar as permissões continuamente

Registre as alterações nos perfis e permissões de identidade e implemente alertas quando as barreiras de proteção de detecção identificarem desvios do estado de configuração esperado. Use ferramentas agregadas e de identificação de padrões para revisar sua coleção centralizada de eventos e refinar as permissões conforme necessário.

Selecione, avalie e melhore continuamente as métricas da sua plataforma

Para permitir operações bem-sucedidas da plataforma, estabeleça e revise rotineiramente métricas abrangentes. Garanta que elas estejam alinhadas às metas organizacionais e às necessidades das partes interessadas. Acompanhe as métricas de performance e melhoria da plataforma e combine parâmetros operacionais, como patch, backup e conformidade, usando indicadores de capacitação da equipe e adoção de ferramentas.

Use a [observabilidade CloudWatch entre contas](#) para um gerenciamento eficiente de métricas. Esse serviço simplifica a agregação e a visualização de dados para permitir decisões informadas e aprimoramentos direcionados. Use essas métricas como indicadores de sucesso e impulsionadores de mudanças para promover um ambiente de melhoria contínua.

Arquitetura de dados

Projete e desenvolva uma arquitetura de dados e analytics adequada à finalidade.

Uma [arquitetura](#) de dados e analytics [bem projetada](#) é essencial para obter insights acionáveis. Ao projetar e desenvolver uma arquitetura de dados e analytics adequada à finalidade, as organizações reduzem a complexidade, o custo e a dívida técnica, ao mesmo tempo em que obtêm insights valiosos de seus volumes de dados cada vez maiores. Ao se alinharem aos princípios do AWS CAF, as empresas podem criar uma arquitetura de dados que se integre perfeitamente à plataforma existente. Esse alinhamento posiciona as organizações para capitalizar as vantagens oferecidas pelas tecnologias modernas de processamento e analytics de dados.

A arquitetura de dados e analytics é o esquema dos recursos de uma organização para extrair valor dos dados. Ela ajuda a organização a obter novos insights de negócios e é um catalisador para o crescimento dos negócios. Para atender às necessidades de negócios, uma arquitetura de dados moderna deve se alinhar às metas de negócios de curto e longo prazo e ser exclusiva para os requisitos culturais e contextuais da organização. No mundo atual, a implementação e a adoção bem-sucedidas de uma arquitetura de dados e analytics são baseadas no princípio de fornecer os dados certos no momento certo para o consumidor certo.

Isso é obtido planejando e organizando como os ativos de dados de uma organização são modelados, física ou logicamente, como os dados são protegidos e como esses modelos de dados interagem entre si para resolver problemas de negócios, derivar padrões desconhecidos e gerar insights.

Iniciar

Definir recurso abrangente

No ambiente de negócios atual, é fundamental que a plataforma moderna de data analytics obtenha valor dos dados para dar suporte a vários domínios da organização. Em vez de adotar uma abordagem de arquitetura de dados única, a [arquitetura de dados moderna](#) deve incluir conjuntos de ferramentas e padrões com propósito específico e otimizados para casos de uso particulares. A arquitetura deve ser capaz de desenvolver e incluir elementos básicos, como data lakes escaláveis, serviços de analytics específicos, acesso unificado a dados e governança unificada.

Organizar zonas de dados

A forma como os dados são organizados e armazenados para acesso rápido e fácil é um aspecto essencial da arquitetura de dados. Isso pode ser feito configurando zonas de dados personalizadas em um data lake. As zonas de dados são categorizadas da seguinte forma:

- Dados brutos coletados de fontes heterogêneas
- Dados selecionados e transformados para apoiar as necessidades analíticas de cada domínio
- Data marts baseados em casos de uso ou produtos para necessidades de relatórios
- Dados expostos externamente com controles de segurança e conformidade

Planejar a agilidade e a democratização dos dados

A eficácia de uma plataforma de analytics depende da velocidade do provisionamento de dados, bem como da democratização dos dados provisionados para consumo. A agilidade do provisionamento de dados é alcançada pela capacidade da arquitetura de dados de adquirir e processar dados de várias maneiras, como em tempo real, quase em tempo real, em lote, em microlote ou híbrido, com base no caso de uso. A democratização dos dados é alcançada definindo fluxos de trabalho de compartilhamento de dados e controle de acesso que são monitorados pelos administradores de dados. A implementação de um marketplace de dados é um dos facilitadores da democratização dos dados.

Definir a entrega segura de dados

Uma arquitetura de dados moderna é uma fortaleza para o mundo exterior em segurança, mas permite o fácil acesso para funcionários ou usuários de dados, conforme definido por suas funções de trabalho, e segue restrições de conformidade, como a [Lei de Portabilidade e Responsabilidade de Seguros de Saúde \(HIPAA\)](#), informações de identificação pessoal (PII), [Regulamento Geral de Proteção de Dados \(RGPD\)](#) e assim por diante. Isso é obtido por meio de métodos de controle de acesso baseado em perfil (RBAC) e controle de acesso baseado em tags (TBAC). Na AWS, as tags são usadas para controlar o acesso aos dados para simplificar o gerenciamento do controle de acesso. Faça isso de acordo com os princípios descritos na perspectiva de segurança do [AWS CAF](#).

Planejar a economia

Os data warehouses tradicionais fornecem computação e armazenamento fortemente acoplados com um alto custo de utilização de recursos. Uma arquitetura moderna desacopla a computação

e o armazenamento e implementa o armazenamento em camadas com base no ciclo de vida dos dados. Por exemplo, na AWS, você pode usar o [Amazon Simple Storage Service \(Amazon S3\)](#) para controlar os custos e desacoplar o armazenamento de dados da computação. As [classes de armazenamento do Amazon S3](#) foram criadas especificamente para fornecer o menor custo de armazenamento para diferentes padrões de acesso. Além disso, as ferramentas de computação da AWS (como [Amazon Athena](#), [AWS Glue](#), [Amazon Redshift](#) e [Amazon SageMaker Runtime](#)) não têm servidor, então você não precisa gerenciar a infraestrutura e paga somente pelo que usa.

Avançado

A arquitetura de dados moderna pode ser aprimorada ainda mais para aumentar a amplitude do uso de dados, desde analytics padrão que apoia funções operacionais e de negócios até recursos mais complexos que apoiam as previsões e os insights, além de ajudar a acelerar a tomada de decisões. Para conseguir isso, a arquitetura oferece suporte aos recursos descritos nas seções a seguir.

Noções básicas sobre engenharia de atributos

A [engenharia de atributos](#) usa machine learning e envolve a configuração de arquivos de atributos ou marts de atributos. As equipes de ciência de dados criam novos atributos (atributos derivados) para modelos de aprendizado supervisionados e não supervisionados e os armazenam em marts de atributos para simplificar a transformação e aumentar a precisão dos dados. As empresas podem reutilizar os atributos em vários modelos de analytics, o que melhora a velocidade de entrada no mercado.

Planejar para desnormalizar conjuntos de dados

A criação de conjuntos de dados ou data marts desnormalizados pode simplificar significativamente os conjuntos de dados para usuários corporativos, disponibilizando prontamente os dados necessários em um único local e aumentando a velocidade do analytics. Se projetado com cuidado, um registro pode ser compatível com vários modelos de uso e reduzir o ciclo de vida geral do desenvolvimento. A governança efetiva de conjuntos de dados desnormalizados também é significativa por dois motivos. A implementação de dados desnormalizados pode criar um grande número de conjuntos de dados redundantes, o que pode se tornar um desafio de gerenciar em grande escala. Além disso, esses conjuntos de dados poderão ser cada vez mais difíceis de reutilizar se não forem modelados corretamente.

Portabilidade e escalabilidade do projeto

As grandes organizações raramente têm todas as suas aplicações e usuários em uma única plataforma de dados. Seus armazenamentos de dados e aplicações são normalmente distribuídos em plataformas legadas on-premises e na nuvem, dificultando que as equipes de analytics misturem e mesquem dados. Recomendamos que você coloque os dados em contêineres com base em características como domínio, geografia, casos de uso de negócios, e assim por diante. Essa containerização aumenta a portabilidade entre várias plataformas e aplicações e oferece suporte a um consumo mais eficiente. Segmentar dados em contêineres e expô-los por meio de APIs ajuda você a escalar sua arquitetura de dados com mais facilidade. Ela permite o fluxo de dados híbrido de ponta a ponta e ajuda as aplicações on-premises e baseadas na nuvem a funcionarem sem problemas.

Excel

À medida que uma arquitetura de analytics moderna é desenvolvida dentro de uma organização, é importante gerenciar essa mudança introduzindo conceitos reutilizáveis. Esses conceitos aumentam a durabilidade e a adoção, mantendo os custos sob controle. Alguns dos conceitos a serem considerados são analisados nas seções a seguir.

Projetar um framework configurável

As organizações geralmente criam vários modelos complexos para atender às suas necessidades de negócios exclusivas. Esses modelos exigem a criação de vários pipelines de dados e recursos projetados. Com o tempo, isso cria uma redundância significativa e aumenta os custos operacionais. A criação de um framework que incorpora um conjunto de modelos básicos configuráveis e orientados por parâmetros reduz o tempo de desenvolvimento e os custos operacionais. O mecanismo de analytics pode implementar esses modelos configuráveis para fornecer a saída desejada.

Planejar criar um mecanismo analítico unificado

Os problemas de negócios são únicos e geralmente exigem tecnologias personalizadas para atender aos requisitos, resultando em vários mecanismos analíticos em uma organização. Projetar e desenvolver uma interface unificada de mecanismo analítico baseada em IA que pode ser compatível com vários paradigmas de programação simplifica o uso e reduz os custos.

Definir DataOps

A maioria dos profissionais de dados dedica uma quantidade significativa de tempo à execução de operações de dados, como localizar os dados certos, transformar, modelar e assim por diante. Ter operações de dados ágeis (DataOps) pode aprimorar significativamente a arquitetura de dados ao eliminar os silos de engenheiros de dados, cientistas de dados, proprietários de dados e analistas. O DataOps permite uma melhor comunicação entre as equipes, reduz o tempo de ciclo e garante a alta qualidade dos dados. As arquiteturas de dados e analytics passaram por várias transformações ao longo do tempo devido às mudanças nas necessidades de negócios e aos avanços tecnológicos. Uma organização deve se esforçar para desenvolver, implementar e manter uma arquitetura de dados e analytics que evolua com o tempo e apoie seus negócios.

Engenharia de dados

Automatize e orquestre fluxos de dados em toda a sua organização.

Use metadados para automatizar [pipelines](#) que processam dados brutos e geram saídas otimizadas. Aproveite as barreiras de proteção de arquitetura e os controles de segurança existentes, conforme definido na arquitetura da plataforma do AWS CAF e nos recursos de engenharia da plataforma, bem como na perspectiva de operações. Trabalhe com a equipe de capacitação de engenharia de plataforma para desenvolver [esquemas](#) reutilizáveis para padrões comuns que simplificam a implantação do pipeline.

Iniciar

Implantar um data lake

Estabeleça recursos básicos de armazenamento de dados usando soluções de armazenamento adequadas para dados estruturados e não estruturados. Isso permite que você colete e armazene dados de várias fontes e os torna acessíveis para processamento e análise adicionais. O armazenamento de dados é um componente essencial de uma estratégia de engenharia de dados. Uma arquitetura de armazenamento de dados bem projetada permite que as organizações armazenem, gerenciem e acessem seus dados de forma eficiente e econômica. A AWS oferece uma variedade de serviços de armazenamento de dados para atender às necessidades específicas dos negócios.

Por exemplo, você pode estabelecer recursos básicos de armazenamento de dados usando o [Amazon Simple Storage Service \(Amazon S3\)](#) para armazenamento de objetos, o [Amazon Relational Database Service \(Amazon RDS\)](#) para bancos de dados relacionais e o [Amazon Redshift](#) para data warehousing. Esses serviços ajudam você a armazenar dados de forma segura e econômica, além de torná-los facilmente acessíveis para processamento e análise adicionais. Recomendamos que você também implemente as práticas recomendadas de armazenamento de dados, como particionamento e compactação de dados, para melhorar a performance e reduzir custos.

Desenvolver padrões de ingestão de dados

Para automatizar e orquestrar fluxos de dados, estabeleça processos de ingestão de dados para coletar dados de diversas fontes, incluindo bancos de dados, arquivos e APIs. Seus processos de ingestão de dados devem apoiar a agilidade dos negócios e levar em consideração os controles de governança.

O orquestrador deve ser capaz de executar serviços baseados em nuvem e fornecer um mecanismo de agendamento automatizado. Ele deve oferecer opções para links condicionais e dependências entre tarefas, além de recursos de pesquisa e tratamento de erros. Além disso, ele deve se integrar perfeitamente aos sistemas de alerta e monitoramento para garantir que os pipelines funcionem sem problemas.

Alguns mecanismos de orquestração conhecidos incluem:

- A orquestração baseada em tempo inicia um fluxo de trabalho em um intervalo recursivo e em uma frequência definida.
- A orquestração baseada em eventos inicia um fluxo de trabalho com base na ocorrência de um evento, como a criação de um arquivo ou uma solicitação de API.
- A pesquisa implementa um mecanismo em que uma tarefa ou fluxo de trabalho chama um serviço (por exemplo, por meio de uma API) e espera por uma resposta definida antes de prosseguir para a próxima etapa.

O design da arquitetura moderna enfatiza o aproveitamento dos serviços gerenciados que simplificam o gerenciamento da infraestrutura na nuvem e reduzem a carga sobre os desenvolvedores e as equipes de infraestrutura. Essa abordagem também se aplica à engenharia de dados. Recomendamos que você use serviços gerenciados, quando aplicável, para criar pipelines de ingestão de dados para acelerar seus processos de engenharia de dados. Dois exemplos desses tipos de serviços são o Amazon Managed Workflows for Apache Airflow (Amazon MWAA) e AWS Step Functions:

- O Apache Airflow é uma ferramenta de orquestração conhecida para criar, programar e monitorar fluxos de trabalho de forma programática. A AWS oferece o [Amazon Managed Workflows for Apache Airflow \(Amazon MWAA\)](#) como um serviço gerenciado que permite que os desenvolvedores se concentrem na criação em vez de no gerenciamento da infraestrutura da ferramenta de orquestração. O Amazon MWAA facilita a criação de fluxos de trabalho usando scripts Python. Um grafo acíclico direcionado (DAG) representa um fluxo de trabalho como uma coleção de tarefas de uma forma que mostra as relações e dependências de cada tarefa. Você pode ter quantos DAGs quiser, e o Apache Airflow os executará de acordo com os relacionamentos e as dependências de cada tarefa.
- O [AWS Step Functions](#) ajuda os desenvolvedores a criar um fluxo de trabalho visual de baixo código para automatizar os processos de TI e de negócios. Os fluxos de trabalho que você cria com o Step Functions são chamados de máquinas de estado, e cada etapa do seu fluxo de trabalho é chamada de estado. Você pode usar o Step Functions para criar fluxos de trabalho para

o tratamento de erros incorporado, a passagem de parâmetros, as configurações de segurança recomendadas e o gerenciamento de estado. Isso reduz a quantidade de código que você precisa escrever e manter. As tarefas executam o trabalho em coordenação com outro serviço da AWS ou aplicação que você hospeda on-premises ou em um ambiente de nuvem.

Acelerar o processamento de dados

O processamento de dados é uma etapa crucial para entender as grandes quantidades de dados coletados pelas organizações modernas. Para começar com o processamento de dados, a AWS oferece serviços gerenciados, como o [AWS Glue](#), que fornece recursos robustos de extração, transformação e carregamento (ETL). As organizações podem usar esses serviços para começar a processar e transformar dados brutos, incluindo limpeza, normalização e agregação de dados para prepará-los para análise.

O processamento de dados começa com técnicas simples, como agregação e filtragem, para realizar as transformações iniciais dos dados. À medida que as necessidades de processamento de dados evoluem, você pode implementar processos ETL mais avançados que permitem extrair dados de várias fontes, transformá-los para atender às suas necessidades específicas e carregá-los em um data warehouse ou banco de dados centralizado para análise unificada. Essa abordagem garante que os dados sejam precisos, completos e estejam disponíveis para análise em tempo hábil.

Ao usar serviços gerenciados da AWS para processamento de dados, as organizações podem se beneficiar de um nível mais alto de automação, escalabilidade e economia. Esses serviços automatizam muitas tarefas rotineiras de processamento de dados, como descoberta de esquemas, criação de perfil de dados e transformação de dados, além de liberar recursos valiosos para atividades mais estratégicas. Além disso, esses serviços são escalados automaticamente para suportar volumes crescentes de dados.

Fornecer serviços de visualização de dados

Encontre maneiras de disponibilizar dados para tomadores de decisão que usam a visualização de dados para interpretar dados de forma significativa e rápida. Por meio de visualizações, você pode interpretar padrões e aumentar o engajamento de um conjunto diversificado de partes interessadas, independentemente de suas habilidades técnicas. Uma boa plataforma permite que as equipes de engenharia de dados provisionem recursos que fornecem visualização de dados de forma rápida e com pouca sobrecarga. Você também pode fornecer recursos de autoatendimento usando ferramentas que podem consultar facilmente armazenamentos de dados sem a necessidade de experiência em engenharia. Considere o uso de ferramentas integradas que possam fornecer

inteligência comercial sem servidor por meio de recursos visuais de dados e painéis interativos, e que possam usar linguagem natural para consultar dados de backend.

Avançado

Implementar processamento de dados quase em tempo real

O processamento de dados é um componente essencial de qualquer pipeline de engenharia de dados, o que permite que as organizações transformem dados brutos em insights significativos. Além do processamento em lote tradicional, o processamento de dados em tempo real tornou-se cada vez mais importante no ambiente de negócios acelerado de hoje. O processamento de dados em tempo real permite que as organizações respondam aos eventos à medida que eles ocorrem e melhora a tomada de decisões e a eficiência operacional.

Validar a qualidade dos dados

A qualidade dos dados afeta diretamente a precisão e a confiabilidade dos insights e decisões derivados dos dados. A implementação de processos de validação e limpeza de dados é essencial para garantir que você use dados confiáveis e de alta qualidade para análise.

A validação de dados envolve a verificação da precisão, a integridade e a consistência dos dados, comparando-os com regras e critérios predefinidos. Isso ajuda a identificar quaisquer discrepâncias ou erros nos dados e garante que eles sejam adequados à finalidade. A limpeza de dados envolve a identificação e correção de quaisquer imprecisões, inconsistências ou duplicações nos dados.

Ao implementar processos e ferramentas de qualidade de dados, as organizações podem melhorar a precisão e a confiabilidade dos insights derivados dos dados, resultando em melhor tomada de decisão e eficiência operacional. Isso não apenas melhora o desempenho da organização, mas também aumenta a confiança das partes interessadas nos dados e nas análises produzidas.

Comprovação de serviços de transformação de dados

A transformação de dados prepara os dados para modelos avançados de analytics e machine learning. Ela envolve o uso de técnicas como a normalização, o aprimoramento e a deduplicação de dados para garantir que os dados estejam limpos, consistentes e prontos para análise.

- A normalização de dados envolve organizar os dados em um formato padrão, eliminar redundâncias e garantir que os dados sejam consistentes em diferentes fontes. Isso facilita a

análise e a comparação de dados de várias fontes e permite que as organizações obtenham uma compreensão mais abrangente de suas operações.

- O aprimoramento de dados envolve potencializar dados existentes com informações adicionais de fontes externas, como dados demográficos ou tendências de mercado. Isso fornece insights valiosos sobre o comportamento dos clientes ou as tendências do setor que podem não ser evidentes apenas nas fontes de dados internas.
- A deduplicação envolve identificar e remover entradas de dados duplicadas e garantir que os dados estejam precisos e livres de erros. Isso é especialmente importante ao lidar com grandes conjuntos de dados, em que até mesmo uma pequena porcentagem de duplicação pode distorcer os resultados da análise.

Ao usar técnicas avançadas de transformação de dados, as organizações garantem que seus dados sejam de alta qualidade, precisos e estejam prontos para análises mais complexas. Isso leva a uma melhor tomada de decisão, maior eficiência operacional e uma vantagem competitiva no mercado.

Habilitar a democratização de dados

Promova uma cultura de democratização de dados, tornando os dados acessíveis, compreensíveis e úteis para todos os funcionários. A democratização de dados ajuda os funcionários a tomar decisões baseadas em dados e contribui para a cultura orientada por dados da organização. Isso significa romper os silos e criar uma cultura em que os dados sejam compartilhados e usados por todos os funcionários para impulsionar a tomada de decisões.

No geral, a democratização dos dados consiste em criar uma cultura em que os dados sejam valorizados, acessíveis e compreensíveis por todos na organização. Ao permitir a democratização dos dados, as organizações promovem uma cultura baseada em dados que impulsiona a inovação, melhora a tomada de decisões e, por fim, leva ao sucesso dos negócios.

Excel

Fornecer orquestração baseada em UI

Para criar organizações que sejam ágeis e usem abordagens eficazes, é importante planejar uma plataforma de orquestração moderna que seja usada por recursos de desenvolvimento e operações em todas as linhas de negócios. O objetivo é desenvolver, implantar e compartilhar fluxos de trabalho e pipelines de dados sem depender de uma única equipe, tecnologia ou modelo de suporte. Isso

é obtido por meio de recursos como a orquestração baseada em interface de usuário. Recursos como a interação de arrastar e soltar permitem que os usuários com pouca experiência técnica criem DAGs e fluxos de dados de máquinas de estado. Esses componentes podem então gerar um código executável que orquestra pipelines de dados.

O DataOps ajuda a superar as complexidades do gerenciamento de dados e garante um fluxo de dados contínuo em todas as organizações. Uma abordagem baseada em metadados garante a qualidade e a conformidade dos dados de acordo com as exigências da sua organização. O investimento em conjuntos de ferramentas como microsserviços, containerização e funções sem servidor melhora a escalabilidade e a agilidade.

Contar com as equipes de engenharia de dados para gerar valor dos dados e deixar as tarefas diárias de infraestrutura para a automação permite que as organizações alcancem a excelência em automação e orquestração. O monitoramento e o registro em log quase em tempo real das tarefas de gerenciamento do fluxo de dados apoiam ações imediatas de remediação e melhoram a performance e a segurança do pipeline de fluxo de dados. Esses princípios ajudam a alcançar escalabilidade e performance, ao mesmo tempo em que garantem um modelo seguro de compartilhamento de dados e preparam as organizações para o sucesso no futuro.

Integrar o DataOps

O DataOps é uma abordagem moderna à engenharia de dados que enfatiza a integração dos processos de desenvolvimento e operações para agilizar a criação, os testes e a implantação do pipeline de dados. Para implementar as práticas recomendadas do DataOps, as organizações usam a infraestrutura como código (IaC) e ferramentas de integração e entrega contínuas (CI/CD). Essas ferramentas têm suporte para a criação, os testes e a implantação automatizados de pipelines, o que melhora significativamente a eficiência e reduz os erros. As equipes do DataOps trabalham com equipes de capacitação de engenharia de plataforma para criar essas automações, para que cada equipe possa se concentrar no que faz de melhor.

A implementação de metodologias DataOps ajuda a promover um ambiente colaborativo para engenheiros de dados, cientistas de dados e usuários corporativos, além de permitir o rápido desenvolvimento, a implantação e o monitoramento de pipelines de dados e soluções de analytics. Essa abordagem fornece uma comunicação e colaboração mais integradas entre as equipes, o que leva a uma inovação mais rápida e melhores resultados.

Para aproveitar ao máximo os benefícios do DataOps, é importante simplificar os processos de engenharia de dados. Isso é obtido usando as práticas recomendadas das equipes de engenharia da plataforma, incluindo revisão de código, integração contínua e testes automatizados. Ao implementar

essas práticas, as organizações garantem que os pipelines de dados sejam confiáveis, escaláveis e seguros e que atendam às necessidades das partes interessadas comerciais e técnicas.

Provisionamento e orquestração

Crie, gerencie e distribua catálogos de produtos de nuvem aprovados para os usuários.

Provisionar a infraestrutura de forma consistente, escalável e repetível torna-se mais desafiador à medida que sua organização cresce. [O provisionamento e a orquestração](#) otimizados ajudam você a atingir uma governança consistente e requisitos de conformidade, ao mesmo tempo que permitem que os usuários implantem somente produtos de nuvem aprovados.

A reutilização de produtos pré-aprovados em sua organização permite que seus desenvolvedores criem aplicações de forma mais rápida e consistente, atendendo aos requisitos de segurança e governança de sua organização.

Início

Implantar um modelo hub-and-spoke de catálogo

Os ativos de software que são gerenciados em um catálogo de serviços como portfólios são compartilhados com usuários em uma ou mais contas em um hub-and-spoke padrão. Você pode usar um marketplace privado e ofertas privadas para organizar uma variedade de soluções de terceiros e distribuí-las com seus modelos de infraestrutura como código (IaC).

Para permitir que seus criadores consumam produtos pré-aprovados, defina um processo para revisar, aprovar e publicar esses produtos para seus usuários. Comece projetando e implementando um repositório gerenciado de forma centralizada que contenha esses produtos pré-aprovados. Crie um sistema que conceda acesso às licenças e aos produtos desse repositório quando os usuários da sua organização precisarem consumir cada produto.

Permita que os criadores da sua organização enviem produtos para aprovação no mecanismo de publicação para que eles sejam disponibilizados para todos os usuários da sua organização após serem aprovados.

Criar modelos para reutilização

Depois de codificar os modelos de IaC para suas soluções e definir seu hub-and-spoke modelo, você deve definir duas categorias de modelos para cada conta spoke: provisionada/aplicada e disponível para consumo. Os modelos provisionados/aplicados são provisionados diretamente da

conta gerencial para a conta de cada membro como recursos básicos. Os modelos disponíveis para consumo estão disponíveis para os criadores navegarem e provisionarem de forma autônoma.

Aplicar parâmetros padrão para reutilização

Implemente modelos de IaC que incluam parâmetros padrão que seus criadores possam pré-selecionar. Isso permite que os criadores se alinhem à governança sem precisar avaliar os detalhes de cada parâmetro e evita que façam escolhas incorretas. Essa abordagem expõe somente o que é necessário para a configuração. Por exemplo, o [AWS Service Catalog](#) implementa essa abordagem com um recurso de restrição que controla as regras aplicadas a um produto em um portfólio específico. Essa personalização é pré-configurada quando a equipe de criadores usa o provisionamento de modelos por autoatendimento.

Estabelecer um processo de aprovação

Os usuários devem poder enviar solicitações para acessar um produto para o qual não foram aprovados se tiverem uma justificativa comercial para usar o produto. Crie um sistema de notificação que informe aos usuários quando as atualizações dos produtos que estão usando estão disponíveis, para que eles possam estar em conformidade com as atualizações de segurança mais recentes.

Estabeleça um fluxo de trabalho para que os construtores enviem novos produtos para análise por meio do portal de autoatendimento. Os criadores podem usar o portal para definir o público do produto e identificar os grupos de usuários que devem ter acesso ao produto. Para cada envio, use seus processos definidos para revisar, aprovar e publicar o produto no portal de autoatendimento.

Avançado

Criar um portal de autoatendimento

Crie um portal de autoatendimento para distribuir, navegar e consumir produtos de nuvem aprovados. Os usuários da organização podem usar esse portal para pesquisar os produtos de que precisam para criar sua infraestrutura e implantar aplicações em seu ambiente. Estabeleça limites de permissões para usuários que tenham acesso aos produtos no portal e defina limites no número de vezes que um usuário pode consumir produtos licenciados. Defina um conjunto básico de recursos que podem ser provisionados diretamente ou disponibilizados como um modelo de autoatendimento em cada uma de suas contas spoke, pois as contas são criadas usando soluções como [Customizações do AWS Control Tower](#).

Habilitar um marketplace privado

Um mercado privado fornece um catálogo organizado de produtos adquiridos (software, dados e serviços profissionais) e é implementado em um hub-and-spoke padrão (com uma conta de gerenciamento e várias contas de membros) para que as contas spoke possam assinar somente o software aprovado. Essa governança de produtos ajuda a controlar os custos de software e otimiza as revisões legais e contratuais. Crie um marketplace privado no nível da conta gerencial para servir como o hub primário.

Gerenciar os direitos

Habilite controles que permitam que somente usuários e workloads autorizados consumam uma licença dentro dos limites definidos pelo fornecedor. Isso ajuda a reduzir o risco de auditorias caras e ajustes inesperados de licenciamento.

Excel

Integrar com sistemas de compras

Complemente seus processos de compras existentes integrando-os ao [AWS Marketplace](#). Isso é feito estendendo seus sistemas de compras (Coupa ou SAP Ariba) para um marketplace privado para que seus usuários possam acompanhar os processos existentes de compras e aprovação para obter o software. Crie as permissões apropriadas gerenciadas pelo IAM, use-as AWS Marketplace para gerar as informações necessárias para configurar sua solução de compras e configure sua solução de compras para concluir a integração. Por exemplo, você pode [configurar um punchout](#), anexar pedidos de compra às suas AWS faturas e, em seguida, alinhar seus processos de aquisição para usar as soluções de provisionamento padrão.

Permita que seus criadores acessem os produtos pré-aprovados por meio de uma API interna, para que os usuários possam incorporar os produtos em suas aplicações ou criar seus próprios portais personalizados para que suas equipes consumam os produtos. Integre o processo de envio e publicação para criar novos produtos e permita que os usuários solicitem novas licenças e acesso aos produtos por meio APIs de.

Integrar com suas ferramentas de ITSM

Se aplicável, [conecte-se às ferramentas de gerenciamento de serviços de TI \(ITSM\)](#) e automatize todas as atualizações em seu banco de dados de gerenciamento de configuração (CMDB).

Estabeleça processos e mecanismos para avaliar os produtos que sua organização usa. Estabeleça um mecanismo para informar aos usuários sobre produtos pré-aprovados que eles precisam atualizar para garantir a conformidade. Use suas ferramentas de ITSM para analisar seu ambiente e enviar atualizações de segurança e conformidade para produtos em toda a organização quando atualizações críticas forem necessárias.

Implemente um sistema de gerenciamento do ciclo de vida e de distribuição de versões

Mantenha versões dos modelos de IaC e versões de serviços provisionados dos modelos durante todo o ciclo de vida de desenvolvimento. Você pode usar o hub-and-spoke modelo implementado em seu catálogo para definir se uma atualização forçada é necessária em nível de spoke (por exemplo, se versões simultâneas estiverem disponíveis para provisionamento de autoatendimento) e quais versões precisam ser marcadas como obsoletas. O uso de um hub-and-spoke catálogo também ajuda a gerenciar a auditoria e a distribuição de novas versões, conforme necessário.

Desenvolvimento de aplicações modernas

Crie aplicações nativas da nuvem bem arquitetadas.

As [práticas modernas de desenvolvimento de aplicações](#) são essenciais para que as organizações criem aplicações nativas da nuvem bem arquitetadas e permaneçam competitivas. As empresas podem usar tecnologias nativas da nuvem, como [contêineres](#) e computação [sem servidor](#) para criar aplicações escaláveis e ágeis que se adaptam às mudanças nas demandas do mercado. Essas tecnologias permitem que as organizações otimizem a utilização de recursos, reduzam custos e melhorem a performance de suas aplicações.

Ao projetar suas aplicações modernas, desenvolva soluções ágeis para operações e desenvolvimento. Uma aplicação moderna reage automaticamente às mudanças na demanda do cliente e é resiliente a falhas. Os engenheiros podem desenvolver e implantar mudanças rapidamente e monitorar o performance da aplicação. Uma aplicação moderna foi projetada para ser autorrecuperável e capaz de ser escalada para níveis grandes ou pequenos de tráfego, incluindo nenhum tráfego a custo zero, quando necessário.

A criação de aplicações nativas da nuvem bem arquitetadas requer uma compreensão profunda das tecnologias subjacentes e de suas práticas recomendadas. As organizações devem adotar uma arquitetura de microsserviços e projetar suas aplicações para serem modulares e terem acoplamento fraco, permitindo implantação e escalabilidade independentes. Essa abordagem permite que as organizações dividam suas aplicações em componentes menores e mais gerenciáveis que são desenvolvidos, testados e implantados de forma rápida e independente.

Iniciar

Analisar abordagens modernas

Comece investigando contêineres, tecnologias sem servidor e outras abordagens que permitem o desenvolvimento de [microsserviços](#), que aumentam a eficiência dos recursos, ajudam a melhorar a segurança e minimizam as despesas de infraestrutura. Opte por [modernizar](#) suas aplicações corporativas e diferenciadoras existentes para melhorar a eficiência e maximizar o valor de seus investimentos existentes. Considere [redefinir a plataforma](#) (a transição de seus contêineres, bancos de dados ou agentes de mensagens autogerenciados para serviços de nuvem gerenciados) e a [refatoração](#) (novo desenvolvimento de suas aplicações para adotar arquiteturas nativas da nuvem) com base na tomada de decisões baseada em valor.

Quando você atualiza sua aplicação baseada em nuvem existente, uma abordagem bem-sucedida envolve o uso do [padrão strangler fig](#) para decompor progressivamente sua arquitetura em microsserviços. Esse procedimento ajuda na adoção de uma metodologia de aplicação contemporânea, para que você possa obter os benefícios inerentes e demonstrar seu valor para a organização maior. Considere criar suas aplicações como microsserviços distintos que aproveitam arquiteturas [orientadas por eventos](#), quando aplicável. Garanta que sua arquitetura leve em consideração as [cotas de serviço](#) e os recursos físicos imutáveis para evitar afetar a performance ou a confiabilidade da workload.

Adotar recursos de computação nativos da nuvem

Os recursos de computação nativos da nuvem são fundamentais para o desenvolvimento moderno de aplicações. Essa abordagem exige que as organizações considerem como desejam que suas unidades de computação sejam hospedadas e identifiquem a melhor opção para cada caso de uso ou serviço. Por exemplo, o [AWS Lambda](#) oferece um mecanismo sem servidor para executar o código da aplicação e desempenha um papel fundamental nas arquiteturas orientadas por eventos. As funções Lambda são lançadas sob demanda e executadas paralelamente até uma simultaneidade máxima definida, para que possam ser escaladas para realizar uma variedade de tarefas.

Usar containerização

No desenvolvimento de software moderno, gerenciar aplicações e suas dependências tornou-se uma tarefa cada vez mais complexa, especialmente quando você considera a necessidade de manter a consistência em vários ambientes. Para enfrentar esses desafios, as tecnologias de containerização, como o Docker, surgiram como uma solução eficaz para empacotar aplicações e suas dependências. Os contêineres garantem implantações consistentes e reproduzíveis, independentemente do ambiente de runtime da sua aplicação, portanto, o desenvolvimento em seu ambiente local se comporta da mesma maneira que o desenvolvimento de produção no ambiente de nuvem. Essa abordagem reduz os erros que podem ser causados por incompatibilidades no ambiente ou em suas configurações.

Usar bancos de dados modernos

Quando você usa bancos de dados modernos, cada microsserviço em sua aplicação pode usar o banco de dados com propósito específico que atenda aos seus requisitos, o que aumenta a agilidade e a performance e, ao mesmo tempo, reduz os custos. Por exemplo, um microsserviço pode usar um banco de dados NoSQL para obter alto throughput ao armazenar dados de sessão, outro

microserviço pode usar um banco de dados relacional para fazer junções complexas de tabelas e outro microserviço pode usar um banco de dados ledger quântico para rastrear alterações no blockchain.

Bancos de dados modernos oferecem escalabilidade e flexibilidade. Eles também ajudam a fornecer melhor segurança, conformidade e confiabilidade do que os bancos de dados tradicionais. Eles permitem que as organizações armazenem e gerenciem seus dados com mais eficiência e garantem que as aplicações possam acessar os dados certos no momento certo, levando a uma melhor performance e experiência do usuário.

A migração para bancos de dados modernos é um componente essencial do desenvolvimento de aplicações modernas. Ao usar as soluções corretas de armazenamento de dados, as organizações podem otimizar seus recursos de gerenciamento de dados e fornecer aplicações mais eficientes e confiáveis. Ao tornar cada microserviço independente e escolher as tecnologias certas para cada microserviço, as organizações podem otimizar ainda mais seus recursos de dados para alcançar a máxima eficiência e escalabilidade e, ao mesmo tempo, minimizar os custos.

Avançado

Otimizar sua arquitetura moderna

Para obter mais otimizações, refine sua implementação de tecnologias sem servidor e desenvolva arquiteturas que possam ser escaladas e implantadas de forma independente usando serviços da AWS como o [Amazon API Gateway](#) e o [AWS Lambda](#). Implemente a descoberta de serviços usando o [Amazon Route 53](#) e o [AWS Cloud Map](#) para garantir uma comunicação perfeita entre os componentes.

Adote o versionamento, o armazenamento em cache e a limitação de taxa da API para manter a compatibilidade e a performance em diferentes versões da aplicação. Melhore a segurança com o [AWS Identity and Access Management \(IAM\)](#) e políticas de recursos. Isso ajuda a garantir que sua infraestrutura seja protegida e que o acesso seja concedido somente a entidades autorizadas.

Se possível, use serviços sem servidor para executar contêineres sem precisar gerenciar a infraestrutura subjacente. Isso permite que você se concentre no desenvolvimento de suas aplicações principais e permite um melhor gerenciamento e performance de recursos. Também ajuda você a aproveitar ao máximo os benefícios da escalabilidade, flexibilidade e eficiência de custos.

Ao se aprofundar nas complexidades das arquiteturas sem servidor e incorporar essas práticas avançadas, as organizações podem descobrir oportunidades de melhoria e ajuste fino e, por fim,

maximizar o potencial de suas aplicações nativas da nuvem. Essa busca facilita a adoção de padrões de aplicações mais sofisticados que elevam ainda mais a experiência geral do usuário. Também capacita as organizações a se tornarem mais ágeis e eficientes em seus processos de desenvolvimento de software.

Usar tecnologias de malha de serviços

À medida que as organizações adotam cada vez mais uma arquitetura de microsserviços para criar e implantar aplicações, o gerenciamento da complexidade, da segurança e das comunicações entre esses serviços se torna essencial. As tecnologias de malha de serviços, como Istio, Linkerd ou Consul, desempenham um papel fundamental para ajudar a aprimorar a segurança, a observabilidade e a confiabilidade dos microsserviços.

Garantir visibilidade e rastreabilidade

As práticas modernas oferecem maior visibilidade e rastreabilidade no processo de desenvolvimento e facilitam a conformidade com os padrões e as práticas recomendadas do setor. Visibilidade e monitoramento são essenciais para o desenvolvimento moderno de aplicações. A implementação de soluções de monitoramento e registro em log para fornecer insights valiosos sobre a performance das aplicações permite que as organizações identifiquem áreas de melhoria e otimizem suas aplicações. Recomendamos que você trabalhe com suas equipes de engenharia de plataforma para garantir que as ferramentas estejam disponíveis para fornecer visibilidade e monitoramento de ponta a ponta dos erros, da performance e da conformidade da aplicação, para que você possa detectar, diagnosticar e resolver problemas rapidamente.

Excel

Adotar microsserviços

Para muitas organizações, o desenvolvimento de aplicações modernas é sinônimo de sucesso nos negócios. Os microsserviços estão no centro dessa transformação, e as organizações podem se beneficiar da adoção desses avançados padrões de arquitetura.

Os microsserviços oferecem uma arquitetura de aplicações altamente escalável, resiliente e ágil. Ao dividir uma aplicação em serviços pequenos e implantáveis de forma independente, as organizações podem optar por iterar rapidamente em componentes específicos sem afetar outras partes da aplicação. Padrões avançados de resiliência, como disjuntores e anteparos, desempenham um papel crucial na garantia da alta disponibilidade dessas aplicações.

Os [disjuntores](#) atuam como um mecanismo de segurança que evita falhas em cascata, interrompendo ou deslocando temporariamente as comunicações de um serviço não íntegro, para que ele possa se recuperar. Os [anteparos](#) isolam os recursos e limitam o escopo do impacto de possíveis falhas. Juntos, esses padrões criam uma arquitetura robusta que resiste a interrupções imprevistas e mantém a performance ideal.

Outro aspecto crítico da implementação de microsserviços é a adoção de princípios de design orientado ao domínio (DDD). O DDD se concentra em criar uma compreensão compartilhada do domínio comercial e traduzi-la em um design de software bem estruturado. Essa abordagem leva a microsserviços mais coesos e sustentáveis e garante que a aplicação evolua de acordo com as necessidades da organização.

Otimizar a comunicação entre serviços também é vital em uma aplicação baseada em microsserviços. Ao implementar protocolos avançados, como gRPC ou GraphQL, as organizações podem melhorar significativamente a eficiência da comunicação entre os serviços. Esses protocolos oferecem recursos como segurança de tipo, baixa latência e flexibilidade, que ajudam a melhorar a performance geral e a capacidade de manutenção da aplicação.

Uma organização que adota microsserviços fornece um ambiente que promove inovação, agilidade e colaboração. As equipes de desenvolvimento geralmente são organizadas de acordo com as capacidades comerciais e têm um forte foco nas práticas de integração e entrega contínuas (CI/CD). Elas têm a autonomia de tomar decisões, experimentar e iterar rapidamente, e adotam uma cultura de responsabilidade e prestação de contas compartilhadas.

Integração e entrega contínuas

Evolua e melhore os serviços e as aplicações com mais rapidez do que organizações que usam processos tradicionais de desenvolvimento de software e gerenciamento de infraestrutura.

A adoção de práticas de [DevOps](#) com [integração](#) e a [entrega contínuas](#) (CI/CD) promove um processo simplificado, automatizado e eficiente para criar, testar e implantar aplicações. O CI/CD permite a entrega rápida de software, reduz o risco de erros de implantação e garante que as aplicações estejam sempre atualizadas com os recursos e correções de bugs mais recentes. O objetivo principal é evoluir e melhorar as aplicações e os serviços em um ritmo mais rápido, evoluindo com base no uso de processos tradicionais de desenvolvimento de software e gerenciamento de infraestrutura.

Iniciar

Adotar o gerenciamento de componentes de software

O gerenciamento de componentes de software é a prática de gerenciar todos os componentes individuais usados para criar software, incluindo bibliotecas, frameworks, repositórios de código-fonte, módulos, artefatos e dependências de terceiros. Recomendamos que você use um sistema de controle de versão, como o Git ou o Apache Subversion, para gerenciar o código-fonte, permitir a colaboração e manter um histórico das alterações no código. Você pode monitorar alterações e eventos no repositório para automatizar o processo, criar pipelines, gerenciar seu código e integrar seus fluxos de trabalho com serviços adicionais, conforme necessário.

Criar os pipelines de CI/CD.

Os pipelines de CI/CD são conjuntos de instruções automatizadas que são iniciadas por alterações confirmadas no sistema de controle de versão. Eles geralmente incluem instruções para criar a aplicação, executar testes automatizados e implantar código em um ambiente específico. Você pode configurar um pipeline automatizado de CI/CD usando ferramentas como [AWS CodePipeline](#), Jenkins, GitLab ou CircleCI. Também é possível configurá-los diretamente em sistemas de controle de versão compatíveis com a geração de pipeline.

Comece com um pipeline mínimo viável para integração contínua e, em seguida, faça a transição para um pipeline de [entrega contínua](#) que inclua mais ações e etapas. Trate sua configuração de entrega contínua como código. Você pode usar vários pipelines distintos para cada filial e equipe,

então pense nas variáveis de configuração que você precisa configurar e na melhor forma de apoiar as equipes que usarão os pipelines.

Considere as janelas de implantação, em quais dias e horários você deseja implantar seu código. Considere as horas de baixa demanda do seu sistema. Portanto, se você precisar reverter, isso terá o menor impacto sobre seus clientes. Outras práticas recomendadas incluem evitar implantações às sextas-feiras e implementar um congelamento de código durante datas de pico elevado ou antes dos feriados. Considere definir regras sobre a implantação de código quando o autor da confirmação não estiver disponível (por exemplo, em férias). Lembre-se de que as implantações falham, e talvez você precise contar com ajuda externa. Avalie diferentes [métodos de implantação](#), como implantações no local, contínuas, imutáveis e azul/verde. Considere o uso de serviços totalmente gerenciados para fluxos de trabalho de entrega contínua, a fim de aumentar a disponibilidade e a segurança e, ao mesmo tempo, minimizar a complexidade e o gerenciamento.

Implementar testes automatizados

As práticas modernas recomendam o shifting left (aproximar os testes do desenvolvedor e do [IDE](#) e no início do ciclo de vida) para detectar e remediar problemas antes que eles sejam confirmados em um repositório e iniciem um pipeline. Essa prática envolve loops rápidos de feedback com o desenvolvedor, porque os erros são detectados enquanto o desenvolvedor está codificando. O shifting left está associado a custos mais baixos, porque os testes não exigem a execução de pipelines, o que pode resultar em feedback assíncrono e maiores despesas operacionais.

Os testes automatizados detectam erros no início do processo de desenvolvimento e inclui testes de unidade, testes de integração e testes funcionais. Recomendamos que você incentive os [desenvolvedores a usar ferramentas](#) para criar testes de unidade o mais cedo possível e executá-los antes de enviar o código para o repositório central. Além disso, certifique-se de que seus processos automatizados incluam [análise estática de código](#), avaliação comparativa de performance e testes de aplicações de segurança.

Criar documentação

Além de implementar um pipeline de CI/CD para agilizar os fluxos de trabalho de desenvolvimento, você deve manter uma documentação clara e abrangente para garantir a eficácia, a capacidade de manutenção e a escalabilidade contínuas do pipeline. A documentação é um aspecto vital dos pipelines de CI/CD, pois fornece às equipes de desenvolvimento uma compreensão clara do design, dos componentes e dos processos do pipeline. Ao criar a documentação, comece com uma visão geral do pipeline, explique as concessões da arquitetura e do design, descreva as ferramentas

e tecnologias que estão sendo usadas, especifique a configuração e as configurações iniciais, descreva as medidas de segurança e o controle de acesso e inclua informações de solução de problemas e manutenção.

Usar infraestrutura como código

Use ferramentas como Terraform, Ansible ou [AWS CloudFormation](#) para gerenciar a infraestrutura e garantir ambientes consistentes e reproduzíveis. Trate sua infraestrutura como código, acompanhe as alterações na infraestrutura e evite fazer alterações diretamente no console. Defina toda a infraestrutura, incluindo o provisionamento de banco de dados, como código e implante essas alterações usando pipelines. Considere executar a integração do banco de dados como código em pipelines com um pequeno subconjunto de dados de produção limpos. Quando possível, faça as alterações e acompanhe essas alterações no código.

Assim como no código de software, siga estas práticas recomendadas para seu código de infraestrutura:

- Use o controle de versões.
- Faça uso de sistemas de rastreamento de bugs e geração de tíquetes.
- Peça aos colegas que revisem as alterações antes de aplicá-las.
- Estabeleça padrões e designs de código de infraestrutura.
- Teste as alterações na infraestrutura.

Manter e acompanhar métricas padrão

Para manter um alto nível de performance, desenvolva e acompanhe as principais métricas para entender o impacto nos negócios e na integridade de seus pipelines, incluindo:

- Frequência de criação. O número de criações oferece insights sobre a produtividade da sua equipe e a complexidade das alterações.
- Frequência de implantação. Implantações regulares indicam um processo de desenvolvimento ágil e íntegro.
- Tempo de antecedência das alterações. Medir o tempo médio para que as alterações cheguem à produção pode ajudar você a identificar gargalos em seu processo de implantação.
- Tempo médio de processamento do pipeline. O tempo médio da etapa inicial do pipeline até cada etapa subsequente pode ajudar a otimizar seu fluxo de trabalho.

- Volume de alterações de produção. Acompanhar o número de mudanças que chegam à produção pode fornecer insights sobre a estabilidade do seu ambiente de produção.
- Tempo de criação. O tempo médio de criação pode indicar possíveis problemas na base de código ou na infraestrutura.

Avançado

Usar gerenciamento de configuração

As ferramentas de gerenciamento de configuração desempenham um papel fundamental na automação da implantação, da configuração e do gerenciamento de software e infraestrutura. Elas fornecem uma abordagem sistemática para lidar com mudanças e manter o estado desejado de infraestrutura, software e configurações em vários ambientes. Essas ferramentas permitem que os desenvolvedores definam o estado desejado de um sistema usando linguagens declarativas ou imperativas. Em seguida, a ferramenta de gerenciamento de configuração automatiza o processo de aplicação dessas configurações aos sistemas de destino, garantindo consistência e repetibilidade.

Use ferramentas de gerenciamento de configuração para automatizar a implantação, a configuração e o gerenciamento de software e infraestrutura. O Gerenciador de Estados do [AWS Systems Manager](#) é um serviço de gerenciamento de configuração seguro e escalável que automatiza o processo de manter os nós gerenciados e outros recursos da AWS em um estado definido por você.

Integrar monitoramento e registro em log

A integração de soluções de monitoramento e registro em log em pipelines de CD oferece vários benefícios para as equipes de desenvolvimento e para o processo geral de desenvolvimento de software. Essas soluções podem fornecer insights em tempo real sobre a performance da aplicação, permitir a identificação e a resolução mais rápidas de problemas e promover a melhoria contínua para ajudar a garantir que as aplicações permaneçam confiáveis, com performance e escaláveis durante todo o ciclo de vida. Investir em soluções de monitoramento e registro em log é um aspecto fundamental para manter um pipeline de CD robusto e eficiente e, em última análise, contribui para a entrega bem-sucedida de software de alta qualidade.

Criar uma cadência para mesclagem

Confirme ou mescle as alterações de código na ramificação da linha principal (trunk ou principal) pelo menos uma vez ao dia ou, de preferência, várias vezes ao dia após cada tarefa. Essa cadência

leva a várias invocações diárias do pipeline. Um modelo de fluxo de trabalho ramificado baseado em pull se alinha a essa abordagem. Use [sinalizadores de recursos](#), [lançamento oculto](#) e técnicas semelhantes para personalizar os recursos que seus clientes usam.

Capturar o comportamento pós-implantação

Depois de uma implantação, capture o comportamento da produção usando testes sintéticos automatizados e sincronize os resultados com o pipeline de entrega contínua para garantir que as ações corretivas ocorram imediatamente. A principal prioridade dos desenvolvedores deve ser corrigir os erros descobertos nos pipelines o mais rápido possível, confirmar as alterações de código no repositório do código-fonte e verificar a resolução de erros no pipeline.

As práticas recomendadas pós-implantação incluem observar os indicadores-chave de performance (KPIs) mais importantes e validar se não há erros no ambiente de produção. Automatize o tratamento de erros e a avaliação de KPIs pós-implantação para quantificar o impacto do seu lançamento. Gere automaticamente métricas de velocidade, segurança e estabilidade que os desenvolvedores podem usar para fazer melhorias. Para obter mais informações, consulte a solução [Painel de Monitoramento de DevOps](#) na AWS.

Excel

Adote práticas e tecnologias de ponta para uma performance ideal. O refinamento contínuo de seus processos de CI/CD ajuda você a melhorar a qualidade do software, a reduzir o tempo de lançamento no mercado e a aumentar a agilidade. Novas técnicas e ferramentas surgem continuamente, o que torna essencial que sua organização se mantenha informada e se adapte para manter uma vantagem competitiva.

Para permanecer adaptável, considere o seguinte:

- Defina tudo como código, incluindo sua aplicação, configuração, infraestrutura, dados, contas e organizações da AWS, pipelines de implantação, redes e controles de segurança e conformidade.
- Crie [pipelines de implantação](#) correspondentes para imagens computacionais, serviços compartilhados e aplicações.
- Considere um modelo do GitOps em que solicitações baseadas em pull iniciam um fluxo de trabalho para implantar alterações comparando o estado da infraestrutura existente com o estado desejado, conforme descrito no código.
- Considere usar pipelines de CD para implantar machine learning (ML), dados, Internet das Coisas (IoT) e outras workloads.

- Assine digitalmente todos os artefatos de criação e armazene-os em um repositório seguro.
- Rastreie a proveniência do software gerando automaticamente uma lista de materiais de software que cria um registro de todos os artefatos versionados e assinados digitalmente que são implantados nos clientes.
- Depois de eliminar todas as atividades manuais em um processo de entrega de software, remova os quadros de revisão manual.

Para aplicações e serviços que automatizaram todo o processo de entrega de software, considere a implantação contínua, em que as equipes implementam mudanças que passam todas as verificações em um pipeline para os clientes em produção. Para uma visualização, consulte o primeiro diagrama em [O que é entrega contínua?](#) no site da AWS.

Integrar tecnologias de IA/ML

A integração das tecnologias de inteligência artificial e machine learning (ML) em pipelines de CI/CD oferece vários benefícios, incluindo os seguintes:

- Geração automatizada de testes
- Priorização inteligente de testes
- Analytics preditivo para detecção de problemas
- Detecção de anomalias e análise da causa raiz
- Revisão de código e garantia de qualidade
- Otimização da implantação

Para obter mais informações, consulte [Adicionar inteligência às suas operações de desenvolvedor](#) no site da AWS.

Adotar práticas de engenharia do caos

A engenharia do caos envolve a injeção intencional de falhas nos sistemas para testar sua capacidade de resistir e se recuperar de eventos inesperados. Ao identificar pontos fracos e abordá-los de forma proativa, as organizações podem melhorar a confiabilidade geral do sistema e minimizar o impacto de possíveis problemas.

Adote práticas de engenharia do caos para testar a resiliência de seus sistemas usando ferramentas como Gremlin, Chaos Monkey ou Litmus. Execute experimentos controlados regularmente para

identificar vulnerabilidades, validar a tolerância a falhas e garantir que sua aplicação lide com falhas inesperadas sem problemas. Essa abordagem proativa ajuda a melhorar a confiabilidade do sistema e contribui para um pipeline de CI/CD mais robusto.

Otimizar a performance

Otimize a performance da sua aplicação continuamente usando ferramentas de criação de perfil, monitoramento em tempo real e ciclos de feedback. Aplique técnicas como as seguintes para garantir que suas aplicações possam lidar com o aumento do tráfego e da demanda:

- Otimização de código
- Criação de perfil
- Monitoramento em tempo real
- Encaminhamentos de feedback
- Armazenamento em cache
- Balanceamento de carga
- Testes de escalabilidade e performance

Implementar a observabilidade avançada

Elevar a observabilidade da sua infraestrutura de nuvem vai além do básico de coletar, agregar e analisar métricas, logs e rastreamentos. Quando a observabilidade é aprimorada com ferramentas como o [Amazon CloudWatch](#) e [AWS X-Ray](#), ela evolui para uma prática estratégica que estimula a entrega contínua e a inovação.

Em um pipeline robusto de CI/CD, a observabilidade avançada permite que você descubra insights, não apenas sobre suas aplicações e infraestrutura, mas também sobre a performance e a integridade de todo o sistema, incluindo o próprio pipeline. Esses insights ajudam você a:

- Identificar, compreender e resolver rapidamente possíveis problemas para melhorar a estabilidade da aplicação e reduzir o tempo de inatividade
- Simplificar seus processos de CI/CD para criar entregas mais rápidas e confiáveis
- Obter insights mais profundos sobre o impacto das alterações e implantações de código para impulsionar a tomada de decisões informada
- Otimizar a utilização de recursos para melhorar a eficiência operacional e a relação custo-benefício

Para elevar a observabilidade:

- Incorpore a observabilidade em todas as camadas de suas aplicações e infraestrutura para criar uma visão abrangente da performance, do comportamento e da integridade de seus sistemas.
- Centralize a coleta, o armazenamento e a análise de dados com ferramentas como o Amazon CloudWatch para unificar seus dados de observabilidade para facilitar o acesso e a interpretação.
- Use AWS X-Ray para rastreamento distribuído para entender a performance de suas aplicações e seus serviços subjacentes.
- Estabeleça loops de feedback para melhoria contínua e use seus dados de observabilidade para impulsionar aprimoramentos iterativos em seus sistemas.

Adotar a observabilidade avançada não significa apenas manter seus sistemas, é um movimento estratégico para alcançar a excelência operacional e impulsionar a inovação contínua em sua organização.

Implementar práticas de GitOps

Implemente as práticas do GitOps para gerenciar as configurações de infraestrutura e aplicações usando um repositório Git como uma única fonte confiável. Essa abordagem simplifica o gerenciamento de alterações, aprimora a rastreabilidade e garante a consistência em todos os ambientes.

Conclusão

Este guia serve como um playbook para a implementação e o gerenciamento bem-sucedidos de uma base para a adoção com êxito da nuvem. Ele analisa como:

- Abordar diretamente os desafios técnicos e as complexidades da [arquitetura da plataforma](#) para estabelecer diretrizes e princípios robustos para seu ambiente de nuvem e os dados que residem nele.
- Desenvolver a [engenharia de plataforma](#) com forte [provisionamento e orquestração](#).
- Permitir o uso de um ambiente de nuvem compatível com várias contas que gerencia e distribui produtos de nuvem aprovados para os usuários de maneira escalável e repetível.
- Apoiar as decisões de [arquitetura de dados](#) com as ferramentas necessárias para que a [engenharia de dados](#) conduza a tomada de decisões baseada em dados.
- Combinar esses recursos com [estratégias modernas de desenvolvimento de aplicações](#) e [processos de CI/CD](#) para promover agilidade, eficiência e inovação em sua organização.
- Criar relacionamentos interfuncionais e receber contribuições de outras perspectivas do AWS CAF em sua própria tomada de decisão para garantir o sucesso de sua plataforma e das equipes por trás dela.

Outras fontes de leitura

Recursos do [AWS Cloud Adoption Framework \(AWS CAF\)](#):

- [E-book](#)
- [Audiolivro](#)
- [Infográfico](#)
- [AWS CAF para inteligência artificial, machine learning e IA generativa](#)
- [Perspectiva de negócios](#)
- [Perspectiva das pessoas](#)
- [Perspectiva de governança](#)
- [Perspectiva de operações](#)
- [Perspectiva de segurança](#)

Recursos adicionais:

- [AWS Centro de Arquitetura da](#)
- [Estudos de caso da AWS](#)
- [AWS Referência geral do](#)
- [AWS Glossário da](#)
- [AWS Centro de Conhecimentos da](#)
- [AWS Recomendações da](#)
- [Soluções de Parceiros da AWS](#) (anteriormente Quick Starts)
- [Documentação de segurança da AWS](#)
- [AWS Biblioteca de Soluções da](#)
- [AWS Training and Certification](#)
- [AWS Well-Architected](#)
- [Guias e whitepapers da AWS](#)
- [Conceitos básicos do AWS](#)
- [Visão geral da Amazon Web Services](#)

Colaboradores

Os colaboradores deste guia incluem:

- Tony Santiago, arquiteto sênior de soluções de parceiros, AWS
- Matias Undurraga, tecnólogo empresarial, AWS
- Alex Torres, arquiteto de soluções sênior, AWS
- Michael Rhyndress, consultor sênior de DevSecOps, AWS
- Alex Livingstone, arquiteto principal de soluções e especialista em CloudOps, AWS
- Bruce Cooper, diretor da SDE, AWS
- Ravinder Thota, consultor sênior de aconselhamento, AWS
- Sausan Yazji, gerente sênior de prática, AWS
- Paul Duvall, diretor de DevSecOps, AWS
- Jeremy Tennant, gerente principal de entrega em nuvem, AWS
- Sneha Shah, líder principal de infraestrutura, AWS
- Sasa Baskarada, líder mundial, AWS Cloud Adoption Framework, 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	—	25 de outubro de 2023

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte [controle de acesso baseado em atributo](#).

serviços abstraídos

Veja [serviços gerenciados](#).

ACID

Veja [atomicidade, consistência, isolamento, durabilidade](#).

migração ativa-ativa

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

migração ativa-passiva

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

AGGREGATE FUNCTION

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

AI

Veja [inteligência artificial](#).

AIOps

Veja [operações de inteligência artificial](#).

anonimização

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

antipadrões

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

controle de aplicações

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para 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 malicioso

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

BCP

Veja [planejamento de continuidade de negócios](#)

gráfico de comportamento

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

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também [endianness](#).

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

Acesso de emergência

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem

ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção [Organizados de acordo com as capacidades de negócios](#) do whitepaper [Executar microsserviços 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

Veja [AWS Cloud Adoption Framework](#).

implantação canário

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

CCoE

Veja [Centro de Excelência da Nuvem](#).

CDC

Veja [captura de dados de alteração](#).

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja [integração e entrega contínuas](#).

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas 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 CCo E](#) no blog de estratégia Nuvem AWS corporativa.

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

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

Esses estágios foram definidos por Stephen Orban na postagem do blog [The Journey Toward Cloud-First & the Stages of Adoption](#) no blog de estratégia Nuvem AWS empresarial. Para obter

informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o [guia de preparação para migração](#).

CMDB

Veja [banco de dados de gerenciamento de configuração](#).

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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 é comumente descrito como um pipeline. CI/CD pode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte [Benefícios da entrega contínua](#). CD também pode significar implantação contínua. Para obter mais informações, consulte [Entrega contínua versus implantação contínua](#).

CV

Veja [visão computacional](#).

D

dados em repouso

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

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte [Classificação de dados](#).

desvio de dados

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

dados em trânsito

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

data mesh

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Veja [linguagem de definição de banco de dados](#).

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta é chamada de administrador delegado para esse serviço. Para obter mais informações e uma lista de serviços compatíveis, consulte [Serviços que funcionam com o AWS Organizations](#) na documentação do AWS Organizations .

implantação

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

ambiente de desenvolvimento

Veja [ambiente](#).

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um [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 [linguagem de manipulação de banco de dados](#).

design orientado por domínio

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

DR

Veja [recuperação de desastres](#).

Deteção da oscilação

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

DVSM

Veja [mapeamento do fluxo de valor de desenvolvimento](#).

E

EDA

Veja [análise exploratória de dados](#).

EDI

Veja [intercâmbio eletrônico de dados](#).

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja [endpoint de serviço](#).

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM). Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte [Criar um serviço de endpoint](#) na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos empresariais (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja [planejamento de recursos empresariais](#).

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

Antecipar-se à falha

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

delimitação de isolamento contra falhas

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

ramificação de recursos

Veja [ramificação](#).

recursos

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

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte [Interpretabilidade do modelo de aprendizado de máquina com AWS](#).

transformação de recursos

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

prompt few shot

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

FGAC

Veja [controle de acesso refinado](#).

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja [modelo de base](#).

modelo de base (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja [restrições geográficas](#).

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

golden image

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais (OUs). Barreiras de proteção preventivas impõem políticas para garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja [alta disponibilidade](#).

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter

o esquema pode ser uma tarefa complexa. [O AWS fornece o AWS SCT](#) para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

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

modernização de historiador

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

dados de hold-out

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de [machine learning](#). Você pode usar dados de hold-out para avaliar a performance do modelo comparando as 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 normal de DevOps lançamento.

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente,

a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

eu

laC

Veja [infraestrutura como código](#).

Política baseada em identidade

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

aplicação ociosa

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

IloT

Veja [Internet das Coisas Industrial](#).

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente

apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das coisas (IoT)

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

interpretabilidade

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

IoT

Veja [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Veja [biblioteca de informações de TI](#).

ITSM

Veja [gerenciamento de serviços de TI](#).

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

informações sobre zonas de pouso, consulte [Configurar um ambiente da AWS com várias contas seguro e escalável](#).

grande modelo de linguagem (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja [controle de acesso baseado em rótulo](#).

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também [endianness](#).

LLM

Veja [grande modelo de linguagem](#).

ambientes inferiores

Veja [ambiente](#).

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da

Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte [Machine learning](#).

ramificação principal

Veja [ramificação](#).

Malware

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

Serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Veja [Programa de Aceleração da Migração](#).

mecanismo

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

conta de membro

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

MES

Veja [sistema de execução de manufatura](#).

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio de uma interface bem definida usando leveza. APIs Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte [Implementação de microsserviços em. AWS](#)

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações,

analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte [discussão sobre fábricas de migração](#) e o [guia do Cloud Migration Factory](#) neste conjunto de conteúdo.

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja [machine learning](#).

modernização

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

avaliação de preparação para modernização

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

aplicações monolíticas (monólitos)

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

MPA

Veja [Avaliação do Portfólio para Migração](#).

MQTT

Veja [Transporte de Telemetria de Enfileiramento de Mensagens](#).

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja [controle de acesso de origem](#).

OAI

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

OCM

Veja [gerenciamento de alterações organizacionais](#).

migração offline

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

OI

Veja [integração de operações](#).

Ola

Veja [acordo de nível operacional](#).

migração online

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

OPC-UA

Veja [Open Process Communications - Unified Architecture](#).

Open Process Communications - Unified Architecture (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (TO)

Sistemas de hardware e software que trabalham com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas de tecnologia da informação (TI) e tecnologia operacional (TO) é o foco principal das transformações da [Indústria 4.0](#).

integração de operações (OI)

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

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de 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 [análise de prontidão operacional](#).

OT

Veja [tecnologia operacional](#).

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja [informações de identificação pessoal](#).

manual

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

PLC

Veja [controlador lógico programável](#).

PLM

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

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pushdown de predicados

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

controle preventivo

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

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais informações, consulte Entidade principal em [Termos e conceitos de perfis](#) na documentação do IAM.

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja [ambiente](#).

controlador lógico programável (PLC)

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

encadeamento de prompts

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

pseudonimização

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

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

Veja [responsável, aprovador, consultado, informado \(RACI\)](#).

RAG

Veja [geração aumentada via recuperação](#).

ransomware

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

Matriz RASCI

Veja [responsável, aprovador, consultado, informado \(RACI\)](#).

RCAC

Veja [controle de acesso por linha e coluna](#).

réplica de leitura

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

Redefinir arquitetura

Veja [7 Rs](#).

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja [7 Rs](#).

Região

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

regressão

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

redefinir a hospedagem

Veja [7 Rs](#).

versão

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

realocar

Veja [7 Rs](#).

redefinir a plataforma

Veja [7 Rs](#).

recomprar

Veja [7 Rs](#).

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja [7 Rs](#).

Retirada

Veja [7 Rs](#).

Geração Aumentada de Recuperação (RAG)

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

alternância

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja [objetivo de ponto de recuperação](#).

RTO

Veja [objetivo de tempo de recuperação](#).

runbook

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

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login no Console de gerenciamento da AWS ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte [Sobre a federação baseada em SAML 2.0](#) na documentação do IAM.

SCADA

Veja [controle de supervisão e aquisição de dados](#).

SCP

Veja [política de controle de serviço](#).

secret

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

segurança desde a concepção

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

controle de segurança

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

hardening da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme avaliado por um [indicador de nível de serviço](#).

modelo de responsabilidade compartilhada

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

SIEM

Veja [sistema de gerenciamento de eventos e informações de segurança](#).

ponto único de falha (SPOF)

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

SLA

Veja [acordo de serviço](#).

SLI

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

SLO

Veja [objetivo de nível de serviço](#).

split-and-seed modelo

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

SPOF

Veja [ponto único de falha](#).

esquema em estrela

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

padrão strangler fig

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

sub-rede

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

controle 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 a performance. Você pode usar o [Amazon CloudWatch Synthetics](#) para criar esses testes.

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja [ambiente](#).

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte [Usando AWS Organizations com outros AWS serviços](#) na AWS Organizations documentação.

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados.

tarefas indiferenciadas

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

ambientes superiores

Veja [ambiente](#).

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

WORM

Veja [gravação única e várias leituras](#).

WQF

Veja [AWS Workload Qualification Framework](#).

gravação única e várias leituras (WORM)

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

Z

exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma [vulnerabilidade zero-day](#).

vulnerabilidade de dia zero

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

prompt zero shot

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

eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt.

Veja também [prompts few-shot](#).

aplicação zumbi

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

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.