AWS Estrutura de adoção da nuvem: perspectiva da plataforma

AWS Orientação prescritiva

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

Table of Contents

AWS Estrutura de adoção da nuvem: perspectiva da plataforma

Amazon Web Services (colaboradores)

Outubro de 2023 (histórico do documento)

A transformação digital é o maior facilitador para os executivos melhorarem a experiência, a inovação e a flexibilidade do cliente. Ele usa aprendizado de máquina (ML), inteligência artificial (IA), 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. Ele pode ajudá-lo a transformar sua organização e, ao mesmo tempo, 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 AWS melhores práticas 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.

AWS O 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 da plataforma, que se concentra em acelerar a entrega de suas cargas de trabalho na nuvem com um ambiente de nuvem híbrida escalável e de nível empresarial.

Introdução

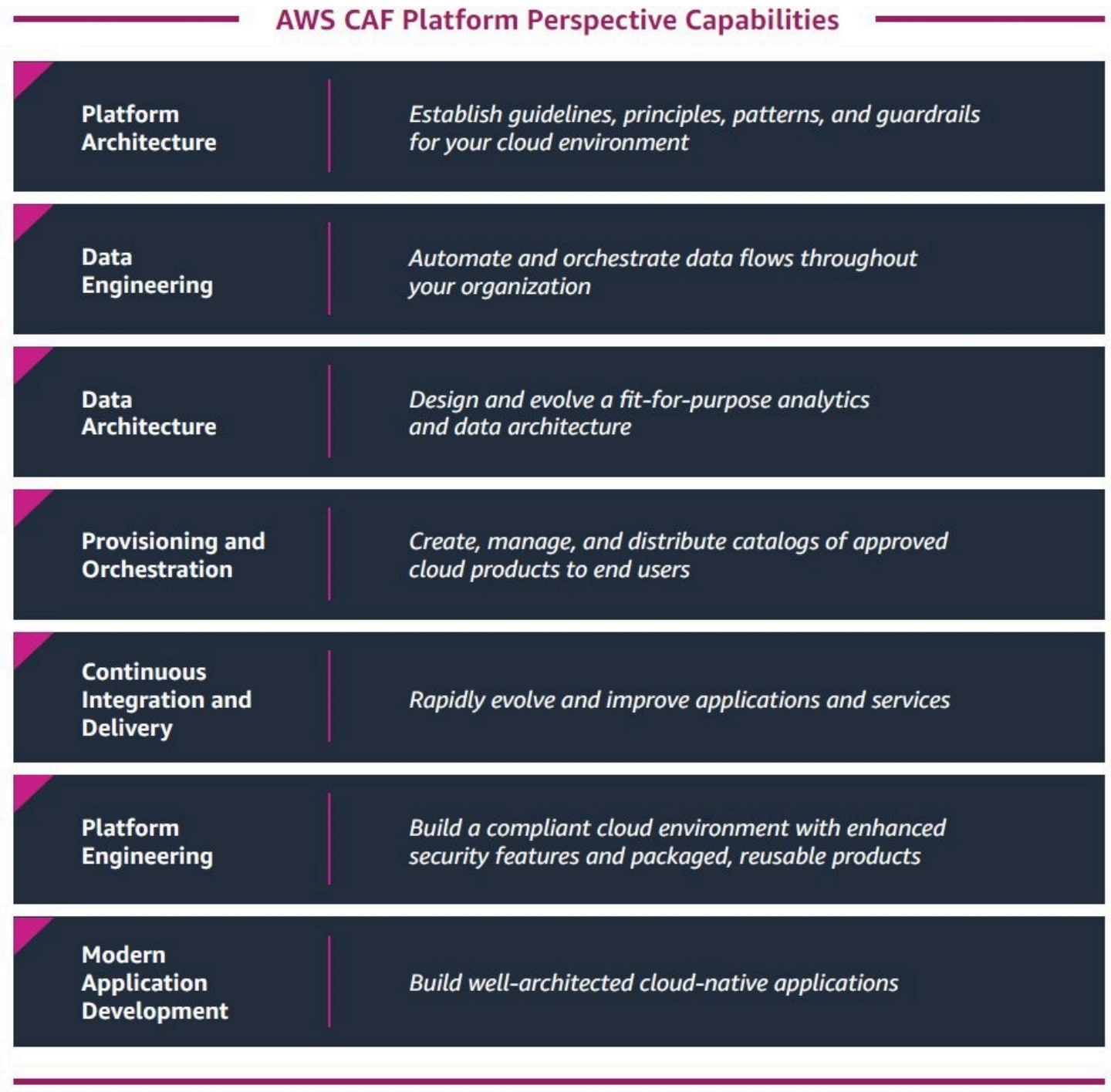
Milhões de clientes, incluindo as startups de crescimento mais rápido, as maiores empresas e as principais organizações governamentais, usam. AWS(Veja histórias de sucesso de clientes no AWS site.) Eles podem migrar e modernizar cargas de trabalho legadas, tornar-se mais orientados por dados, automatizar e otimizar processos de negócios e reinventar modelos operacionais. Eles são capazes de melhorar seus resultados comerciais 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 efetivamente a nuvem para se transformar digitalmente (prontidão organizacional para a nuvem) é reforçada por um conjunto de recursos fundamentais. Uma capacidade é a capacidade organizacional de usar processos para implantar recursos (pessoas, tecnologia e quaisquer outros ativos tangíveis ou intangíveis) para alcançar um resultado específico. O AWS CAF identifica esses recursos 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 da nuvem.

AWS O CAF agrupa suas capacidades em seis perspectivas:

- Negócios
- Pessoas
- Governança
- Plataforma
- Segurança
- Operações

A perspectiva da plataforma se concentra em acelerar a entrega de suas cargas de trabalho 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 típicas incluem o diretor de tecnologia (CTO), líderes de tecnologia, arquitetos e engenheiros.



Esses recursos são discutidos 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 da plataforma
- Engenharia de plataforma
- Arquitetura de dados

- Engenharia de dados
- Provisionamento e orquestração
- Desenvolvimento moderno de aplicativos
- Integração e entrega contínuas (CI/CD)

A perspectiva da plataforma é uma peça fundamental do AWS CAF. É o nexo no qual as decisões tomadas em todas as outras perspectivas convergem para fornecer agilidade e valor aos negócios. As decisões tomadas aqui ajudam ou atrapalham seus objetivos de negócios em um nível fundamental. A perspectiva da plataforma 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 na perspectiva da 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 que suas equipes precisam para criar a plataforma e permitir seu uso em todas as equipes de aplicativos. Lembre-se das pessoas, dos negócios, da governança, da segurança e dos 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.

AWS e a AWS Partner Network fornecem ferramentas e serviços, como workshops e treinamentos, que podem ajudá-lo nessa jornada para implementar e melhorar sua postura de segurança.AWS A Professional Services é uma equipe global de especialistas que pode ajudá-lo a alcançar resultados específicos relacionados à sua transformação na nuvem por meio de uma coleção de ofertas AWS alinhadas ao CAF.

Arquitetura de plataforma

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

Um ambiente de nuvem bem arquitetado ajuda você a acelerar a implementação, reduzir riscos e 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 proteções de melhores práticas para facilitar a autenticação, a segurança, a rede, o registro e o monitoramento. Além disso, você leva em consideração e planeja as cargas de trabalho que talvez precise reter no local devido aos requisitos de latência, processamento de dados ou residência de dados e avalia casos de uso da nuvem híbrida, como explosão da nuvem, backup e recuperação de desastres na nuvem, processamento distribuído de dados e computação de ponta.

Início

Defina uma estratégia de várias contas

Uma boa estratégia de várias contas considera questões de escala e eficiência operacional. Isso significa isolar suas cargas de trabalho 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 cargas de trabalho 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.

Defina controles preventivos

Planeje um ambiente seguro com várias contas com um conjunto incorporado de controles padrão (grades de proteção). Comece a entender e usar um mecanismo, como políticas de controle de serviços (SCPs), para gerenciar o uso de serviços em toda a organização, incluindo Regiões da AWS aqueles 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 (OUs) 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 OUs, as organizações simplificam o processo de solicitação de políticas e permissões apropriadas em toda a infraestrutura de nuvem. OUsAs cargas de trabalho são projetadas especificamente para contas que oferecem suporte a recursos de infraestrutura de aplicativos e garantem que as políticas corretas sejam aplicadas. Use OUs e SCPs ajude a aprimorar a segurança e a conformidade da infraestrutura de nuvem da sua organização, além de garantir a operação tranquila de seus aplicativos e serviços. Em última análise, isso leva a um processo de adoção da nuvem mais eficiente e robusto.

Defina a 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 suportar aplicativos e cargas de trabalho. Uma rede bem projetada fornece alto desempenho consistente e garante operações contínuas em diferentes ambientes.

Ao projetar sua arquitetura de rede, considere se você tem cargas de trabalho que deseja manter no local devido aos requisitos de latência, processamento de dados ou residência de dados. Ao avaliar 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, você pode identificar os principais requisitos para os seguintes aspectos:

- Conectividade de e para a Internet. Esse aspecto envolve o fornecimento de conexões seguras e confiáveis entre seus aplicativos ou cargas de trabalho e a Internet. Essa conectividade é essencial para facilitar o acesso a recursos baseados na web, permitir a comunicação entre usuários e aplicativos 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. Ele 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 VPCs são criados e monitorados. Considere criar esses padrões programaticamente 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 melhores práticas de segurança VPCs ao projetar e implementar a conectividade de rede.

- Conectividade entre sua rede local e seus ambientes de nuvem. Esse aspecto trata da integração de sua infraestrutura local 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 locais e serviços em nuvem simultaneamente para melhorar o desempenho, 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 suporte seus aplicativos e cargas de trabalho 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.

Defina 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 local, recomendamos que você crie arquiteturas de DNS híbridas que usem a infraestrutura de DNS local junto com o DNS na nuvem para quaisquer requisitos de DNS baseados na nuvem. Integre a resolução de DNS com ambientes DNS locais usando endpoints de resolução e regras de encaminhamento. Use zonas hospedadas privadas para armazenar informações sobre como você deseja que o Cloud DNS responda às consultas de um domínio e seus subdomínios em uma ou mais redes.

Defina padrões de marcação

Marcar 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 Cloud Financial Management (CFM) na perspectiva da governança do AWS CAF. Identifique um mecanismo de geração de relatórios que apoie suas práticas contábeis e financeiras, incluindo ações a serem tomadas quando as políticas financeiras forem violadas.

Defina 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 registros produzidos por seus serviços em nuvem em insights acionáveis para a tomada de decisões estratégicas. Priorize o monitoramento dos principais indicadores de desempenho e a configuração de alertas para abordar preventivamente possíveis problemas. Para evitar a proliferação de ferramentas, otimizar custos e se concentrar no que é mais importante para sua organização, incorpore essa estratégia de observabilidade em sua plataforma e aplicativos. Para obter mais orientações, consulte nossa apresentação sobre Desenvolvimento de uma estratégia de observabilidade (AWS re:Invent 2022).

Avançar

Defina controles proativos e de detetive

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

Defina 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.

Defina padrões e princípios

Considere quais padrões de arquitetura serão permitidos em sua organização usando informações dos proprietários de aplicativos e comece a definir planos para 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

Defina padrões de remediação

Considere como anotar e priorizar suas descobertas de proteção de detetive para que elas possam ser corrigidas de acordo com suas estruturas de segurança e conformidade. Planeje usar a automação para detectar o out-of-policy provisionamento de recursos, incluindo aqueles que violam as políticas orçamentárias e de marcação. Identifique os recursos necessários para definir e medir os objetivos de nível 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 adequadamente.

Comunique e refine as 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.

Entenda os recursos de gerenciamento financeiro

As organizações prosperam quando mantêm uma compreensão transparente e abrangente de seu orçamento. Isso os 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 destacarem, facilitando a tomada de decisões informadas, a alocação efetiva de recursos, o controle de custos, a medição 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 AWS Budgetspara 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 tags de alocação de AWS custos e Cost Categories a tags para gerar insights financeiros e transparência ao relatar custos.

Engenharia de plataforma

Crie um ambiente de nuvem multicontas 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. (Veja a perspectiva comercial AWS da CAF.) Ele deve fazer isso sendo flexível o suficiente para se adaptar às demandas de gerenciamento de produtos, rígido o suficiente para aderir às restrições de segurança e rápido 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 embalados 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 melhores práticas, ajuda na governança e ajuda a aumentar a velocidade e a consistência de suas implantações na nuvem. Implemente seus planos de melhores práticas e proteções preventivas e de detetive. 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 locais e na nuvem, bem como entre diferentes contas na nuvem. Implemente a federação entre seu provedor de identidade (IdP) existente e seu ambiente de nuvem para que os usuários possam se autenticar usando suas credenciais de login existentes. Centralize o registro, estabeleça auditorias de segurança entre contas, crie resolvedores de DNS de entrada e saída e obtenha visibilidade de suas contas e proteções no painel.

Avalie e certifique os serviços em nuvem para consumo em alinhamento com os padrões corporativos e o gerenciamento de configurações. Package 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 discutidas 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 AWS whitepaper Estabelecendo sua base na nuvem.

Início

Construa uma landing zone e implante grades de proteção

Ao iniciar sua jornada rumo à engenharia de plataforma madura, você deve primeiro implantar sua landing zone com proteções preventivas e detectivas, conforme definido no recurso de arquitetura da plataforma. As grades de proteção garantem que os padrões organizacionais não sejam violados à medida que os proprietários de aplicativos consomem recursos de nuvem. Com esse mecanismo, você automatiza o fluxo de trabalho de provisionamento de contas para usar várias contas que suportem suas metas de segurança e governança.

Estabelecer autenticação

Implemente gerenciamento de identidade e controle de acesso em todos os ambientes, sistemas, cargas de trabalho e processos de acordo com os padrões ditados na perspectiva de segurança da AWS CAF. Para identidades da força de trabalho, restrinja o uso de usuários AWS Identity and Access Management (IAM) e, em vez disso, confie em um provedor de identidade que permite gerenciar identidades em um local centralizado. Isso facilita o gerenciamento do acesso em vários aplicativos e serviços, porque você está criando, gerenciando e revogando o acesso em um único local. Use os processos existentes para gerenciar a criação, atualização e remoção do acesso para incluir seus AWS ambientes.

Implante 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 rapidamente provisionada 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 conectividade em todo o ambiente usando controles preventivos e reativos.

Colete, agregue e proteja dados de eventos e registros

Use a observabilidade CloudWatch entre contas da Amazon. Ele fornece uma interface unificada para pesquisar, visualizar e analisar métricas, registros e rastreamentos em suas contas vinculadas e elimina os limites da conta.

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

Implemente políticas robustas para proteger dados de registro confidenciais, usando técnicas de mascaramento conforme necessário. Use a agregação de registros para registros de conformidade, segurança e auditoria e garanta o uso de proteções rígidas e construções de identidade para evitar alterações não autorizadas nas configurações de registro.

Estabeleça controles

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

Implemente o gerenciamento financeiro na 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 Explorerde faturamento publicados em AWS Cost and Usage Report.

Avançar

Automação de infraestrutura de construção

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 baseado em função (RBAC) ou controle de acesso baseado em atributos (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 eles. AWS Atualize seus playbooks e runbooks conforme apropriado.

Forneça 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 log locais e centralizados. À medida que suas operações aumentam, a capacidade de sua plataforma de indexar, visualizar e interpretar registros, métricas e rastreamentos é fundamental para transformar dados brutos em insights acionáveis.

Ao correlacionar registros, 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 registros, 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.

Implemente 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 terminais, 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 no Amazon Machine Images (AMIs) e AMIs disponibilizá-las aos consumidores da plataforma em nuvem. Use controles preventivos e de detetive que governem o uso deles. AMIs AMIs deve conter ferramentas que permitam o gerenciamento de EC2 instâncias de longa execução em grande escala, especialmente para cargas de trabalho EC2 mutáveis da Amazon que não consomem AMIs novas regularmente. Você pode usar AWS Systems Managerem

grande escala para automatizar atualizações de agentes, coletar inventário do sistema, acessar EC2 instâncias remotamente e corrigir vulnerabilidades do sistema operacional.

Gerenciar o uso de credenciais

De acordo com a perspectiva de segurança da AWS CAF, implemente funções e credenciais temporárias. Use ferramentas para gerenciar o acesso remoto a instâncias ou sistemas locais 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 aplicativos e senhas de banco de dados, para automatizar a rotação e o gerenciamento de credenciais. Codifique usuários, grupos e funções usando princípios de privilégio mínimo com o IaC e evite a criação manual de contas de identidade usando grades de proteção.

Estabeleça ferramentas de segurança

As ferramentas de monitoramento de segurança devem oferecer suporte ao monitoramento granular da segurança em toda a infraestrutura, aplicativos e cargas de trabalho 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

Crie e distribua construções de identidade com automação

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

Adicione detecção e alertas para padrões anômalos em todos os ambientes

Avalie proativamente os ambientes em busca de vulnerabilidades conhecidas e acrescente 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.

Analise e modele ameaças

Implemente monitoramento e medição contínuos em relação aos benchmarks do setor e de segurança, de acordo com os requisitos da perspectiva da AWS CAF Security. 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 e análise seguros em seus ambientes de várias contas, incluindo a capacidade de correlacionar eventos de várias fontes. Evite alterações nessa configuração com controles e grades de proteção específicos.

Colete, revise e refine as permissões continuamente

Registre as alterações nas funções e permissões de identidade e implemente alertas quando as grades de proteção do detetive detectarem 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, meça e melhore continuamente as métricas da sua plataforma

Para permitir operações bem-sucedidas da plataforma, estabeleça e revise rotineiramente métricas abrangentes. Garanta que eles estejam alinhados às metas organizacionais e às necessidades das partes interessadas. Acompanhe as métricas de desempenho 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 da mudança para promover um ambiente de melhoria contínua.

Arquitetura de dados

Projete e desenvolva uma arquitetura fit-for-purpose de dados e análises.

Uma arquitetura de dados e análise bem projetada é essencial para obter insights acionáveis. Ao projetar e desenvolver uma arquitetura de fit-for-purpose dados e análises, as organizações reduzem a complexidade, o custo e a dívida técnica, ao mesmo tempo em que obtêm informações valiosas 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 análise de dados.

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

Isso é conseguido 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.

Início

Defina a capacidade abrangente

No ambiente de negócios atual, é fundamental que a plataforma moderna de análise de dados obtenha valor dos dados para dar suporte a vários domínios na organização. Em vez de adotar uma abordagem de arquitetura de dados única, a arquitetura de dados moderna deve incluir conjuntos de ferramentas e padrões criados especificamente e otimizados para casos de uso específicos. A arquitetura deve ser capaz de evoluir e incluir elementos básicos, como lagos de dados escaláveis, serviços de análise específicos, acesso unificado a dados e governança unificada.

Organize 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

Planeje a agilidade e a democratização dos dados

A eficácia de uma plataforma de análise 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, 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 mercado de dados é um dos facilitadores da democratização dos dados.

Defina a entrega segura de dados

Uma arquitetura de dados moderna é uma fortaleza para o mundo exterior em segurança, mas permite fácil acesso a 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 (GDPR) e assim por diante. Isso é obtido por meio dos métodos de controle de acesso baseado em função (RBAC) e controle de acesso baseado em tags (TBAC). Ativado 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 da AWS CAF.

Planeje a relação custo-benefício

Os data warehouses tradicionais fornecem computação e armazenamento fortemente acoplados com um alto custo de utilização de recursos. Uma arquitetura moderna separa computação e armazenamento e implementa o armazenamento em camadas com base no ciclo de vida dos dados. Por exemplo, ativado AWS, você pode usar o Amazon Simple Storage Service (Amazon S3) para controlar custos e dissociar 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 AWS computacionais (como Amazon Athena AWS Glue, Amazon Redshift e SageMaker Amazon Runtime) não têm servidor, então você não precisa gerenciar a infraestrutura e paga somente pelo que usa.

Avançar

A arquitetura de dados moderna poderia ser aprimorada ainda mais para aumentar a amplitude do uso de dados, desde análises padrão que oferecem suporte a funções operacionais e comerciais até recursos mais complexos que suportam previsões e insights, além de ajudar a acelerar a tomada de decisões. Para conseguir isso, a arquitetura oferece suporte aos recursos descritos nas seções a seguir.

Entenda a engenharia de recursos

A engenharia de recursos usa aprendizado de máquina e envolve a configuração de lojas de recursos ou mercados de recursos. As equipes de ciência de dados criam novos recursos (atributos derivados) para modelos de aprendizado supervisionados e não supervisionados e os armazenam em mercados de recursos para simplificar a transformação e aumentar a precisão dos dados. As empresas podem reutilizar os recursos em vários modelos de análise, o que melhora a velocidade de entrada no mercado.

Planeje a desnormalização dos conjuntos de dados

A construção 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 da análise. Se projetado com cuidado, um registro pode suportar 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 podem ser cada vez mais difíceis de reutilizar se não forem modelados corretamente.

Portabilidade e escalabilidade do projeto

As grandes organizações raramente têm todos os seus aplicativos e usuários em uma única plataforma de dados. Seus aplicativos e armazenamentos de dados são normalmente distribuídos em plataformas legadas no local e na nuvem, dificultando que as equipes de análise misturem e mesclem dados. Recomendamos que você coloque os dados em contêineres com base em características como domínio, geografia, casos de uso comercial e assim por diante. Essa conteinerização aumenta a portabilidade entre várias plataformas e aplicativos e oferece suporte a um consumo mais eficiente. Segmentar dados em contêineres e expô-los APIs ajuda você a escalar sua arquitetura de dados com mais facilidade. Ele permite o fluxo de end-to-end dados híbrido e ajuda os aplicativos locais e baseados na nuvem a funcionarem sem problemas.

Excel

À medida que uma arquitetura de análise moderna evolui 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 discutidos nas seções a seguir.

Projete uma estrutura configurável

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

Planeje 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 suportar vários paradigmas de programação simplifica o uso e reduz os custos.

Definir DataOps

A maioria dos profissionais de dados gasta uma quantidade significativa de tempo executando operações de dados, como localizar os dados certos, transformar, modelar e assim por diante. Ter

operações de dados ágeis (DataOps) pode aprimorar muito a arquitetura de dados ao eliminar os silos de engenheiros de dados, cientistas de dados, proprietários de dados e analistas. 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 análises passaram por várias transformações ao longo do tempo devido às mudanças nas necessidades comerciais e aos avanços tecnológicos. Uma organização deve se esforçar para desenvolver, implementar e manter uma arquitetura de dados e análises 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 proteções arquitetônicas e os controles de segurança existentes, conforme definido na arquitetura da plataforma 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.

Início

Implemente 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. 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 armazenamento de dados. 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 melhores práticas de armazenamento de dados, como particionamento e compactação de dados, para melhorar o desempenho e reduzir custos.

Desenvolva 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 dutos funcionem sem problemas.

Alguns mecanismos de orquestração populares 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 no qual 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 Amazon Managed Workflows for Apache Airflow (Amazon MWAA) e: AWS Step Functions

- O Apache Airflow é uma ferramenta de orquestração popular para criar, programar e monitorar fluxos de trabalho de forma programática. 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 gerenciar, a infraestrutura da ferramenta de orquestração. O Amazon MWAA facilita a criação de fluxos de trabalho usando scripts Python. Um gráfico 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 DAGs quantas quiser, e o Apache Airflow as executará de acordo com os relacionamentos e dependências de cada tarefa.
- AWS Step Functionsajuda 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 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 tratamento de erros incorporado, passagem de parâmetros, configurações de segurança recomendadas e gerenciamento de estado. Isso reduz a quantidade de código que você precisa escrever e manter. As tarefas executam o trabalho em coordenação com outro AWS serviço ou aplicativo que você hospeda localmente ou em um ambiente de nuvem.

Acelere 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, AWS oferece serviços gerenciados AWS Glue, como o, que fornece recursos poderosos 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 AWS gerenciados 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.

Forneça 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 rapidamente 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 back-end.

Avançar

Implemente o 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.

Valide 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, integridade e 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.

Prove os serviços de transformação de dados

A transformação de dados prepara os dados para modelos avançados de análise e aprendizado de máquina. Ela envolve o uso de técnicas como normalização, enriquecimento e desduplicação 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 enriquecimento de dados envolve o aprimoramento dos dados existentes com informações adicionais de fontes externas, como dados demográficos ou tendências de mercado. Isso fornece informações valiosas sobre o comportamento do cliente ou as tendências do setor que podem não ser evidentes apenas nas fontes de dados internas.
- A desduplicação envolve identificar e remover entradas de dados duplicadas e garantir que os dados sejam precisos e livres de erros. Isso é especialmente importante ao lidar com grandes conjuntos de dados, nos quais 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 prontos para análises mais complexas. Isso leva a uma melhor tomada de decisão, maior eficiência operacional e uma vantagem competitiva no mercado.

Permita a democratização dos dados

Promova uma cultura de democratização de dados, tornando os dados acessíveis, compreensíveis e utilizáveis 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

Forneça 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 orquestração baseada em interface de usuário. Recursos como drag-and-drop interação permitem que usuários com pouco conhecimento técnico construam DAGs e declarem fluxos de dados de máquinas. Esses componentes podem então gerar código executável que orquestra pipelines de dados.

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, conteinerização e funções sem servidor melhora a escalabilidade e a agilidade.

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

Integrar DataOps

DataOps é uma abordagem moderna à engenharia de dados que enfatiza a integração dos processos de desenvolvimento e operações para agilizar a criação, o teste e a implantação do pipeline de dados. Para implementar as DataOps melhores práticas, as organizações usam infraestrutura como código (IaC) e ferramentas de integração contínua e entrega contínua (CI/CD). Essas ferramentas oferecem suporte à criação, teste e implantação automatizados de pipelines, o que melhora significativamente a eficiência e reduz os erros. DataOps as equipes 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 DataOps metodologias ajuda a promover um ambiente colaborativo para engenheiros de dados, cientistas de dados e usuários corporativos, além de permitir o rápido desenvolvimento, implantação e monitoramento de pipelines de dados e soluções de análise. Essa abordagem fornece comunicação e colaboração mais perfeitas 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 melhores práticas 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 se torna mais desafiador à medida que sua organização cresce. O provisionamento e a orquestração simplificados ajudam você a obter uma governança consistente e atender aos requisitos de conformidade, permitindo que os usuários implantem somente produtos de nuvem aprovados.

A reutilização de produtos pré-aprovados em sua organização permite que seus desenvolvedores criem aplicativos de forma mais rápida e consistente, ao mesmo tempo em que atendem 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 mercado privado e ofertas privadas para organizar uma variedade de soluções de terceiros e distribuí-las com sua infraestrutura como modelos de 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 centralmente que contém 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 esses produtos sejam disponibilizados para todos os usuários da sua organização após serem aprovados.

Crie 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 de

gerenciamento 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 construtores 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, AWS Service Catalogimplementa 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.

Estabeleça 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.

Avançar

Crie 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 aplicativos 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 para. AWS Control Tower

Habilite um mercado 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 do produto ajuda a controlar os custos de software e simplifica as revisões legais e contratuais. Crie um mercado privado no nível da conta de gerenciamento para servir como o hub principal.

Gerenciar direitos

Ative controles que permitam que somente usuários e cargas de trabalho 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

Integre com sistemas de compras

Complemente seus processos de aquisição existentes integrando-os em. AWS Marketplace Isso é feito estendendo seus sistemas de compras (Coupa ou SAP Ariba) para um mercado privado para que seus usuários possam acompanhar os processos existentes de aquisição 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 seus aplicativos 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.

Integre 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 distribuição de versões

Mantenha versões dos modelos de IaC e versões de serviços provisionados a partir 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 obsolescentes. 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 aplicativos nativos da nuvem bem arquitetados.

As práticas modernas de desenvolvimento de aplicativos são essenciais para que as organizações criem aplicativos nativos da nuvem bem arquitetados e permaneçam competitivas. As empresas podem usar tecnologias nativas da nuvem, como contêineres e computação sem servidor, para criar aplicativos 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 o desempenho de seus aplicativos.

Ao projetar seus aplicativos modernos, desenvolva soluções ágeis para operações e desenvolvimento. Um aplicativo moderno reage automaticamente às mudanças na demanda do cliente e é resistente a falhas. Os engenheiros podem desenvolver e implantar mudanças rapidamente e monitorar o desempenho do aplicativo. Um aplicativo moderno foi projetado para ser autorrecuperável e capaz de ser escalado para níveis grandes ou pequenos de tráfego, incluindo nenhum tráfego a custo zero, quando necessário.

A criação de aplicativos nativos da nuvem bem arquitetados requer uma compreensão profunda das tecnologias subjacentes e de suas melhores práticas. As organizações devem adotar uma arquitetura de microsserviços e projetar seus aplicativos para serem modulares e fracamente acoplados, permitindo implantação e escalabilidade independentes. Essa abordagem permite que as organizações dividam seus aplicativos em componentes menores e mais gerenciáveis que são desenvolvidos, testados e implantados de forma rápida e independente.

Início

Explore 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 seus aplicativos corporativos e diferenciadores existentes para melhorar a eficiência e maximizar o valor de seus investimentos existentes. Considere a replataforma (a transição de seus contêineres, bancos de dados ou agentes de mensagens autogerenciados para serviços de nuvem gerenciados) e a refatoração (redesenvolvimento de seus aplicativos para adotar arquiteturas nativas da nuvem) com base na tomada de decisões baseada em valor.

Quando você atualiza seu aplicativo baseado 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 construir seus aplicativos 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 o desempenho ou a confiabilidade da carga de trabalho.

Adote recursos de computação nativos da nuvem

Os recursos de computação nativa em nuvem são fundamentais para o desenvolvimento moderno de aplicativos. 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, AWS Lambdaoferece um mecanismo sem servidor para executar o código do aplicativo 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.

Use a conteinerização

No desenvolvimento de software moderno, gerenciar aplicativos e suas dependências se tornou uma tarefa cada vez mais complexa, especialmente quando você considera a necessidade de manter a consistência em vários ambientes. Para enfrentar esses desafios, tecnologias de conteinerização, como o Docker, surgiram como uma solução eficaz para empacotar aplicativos e suas dependências. Os contêineres garantem implantações consistentes e reproduzíveis, independentemente do ambiente de execução do seu aplicativo, 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.

Use bancos de dados modernos

Quando você usa bancos de dados modernos, cada microsserviço em seu aplicativo pode usar o banco de dados específico certo que atenda aos seus requisitos, o que aumenta a agilidade e o desempenho e reduz os custos. Por exemplo, um microsserviço pode usar um banco de dados NoSQL para obter alta taxa de transferência ao armazenar dados de sessão, outro microsserviço pode usar um banco de dados relacional para fazer junções complexas de tabelas e outro

microsserviço pode usar um banco de dados de contabilidade quântica 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 os aplicativos possam acessar os dados certos no momento certo, levando a um melhor desempenho e experiência do usuário.

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

Avançar

Otimize 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 como AWS Amazon API Gateway e.AWS Lambda Implemente a descoberta de serviços usando o Amazon Route 53 e AWS Cloud Mapgaranta uma comunicação perfeita entre os componentes.

Adote o controle de versão, o armazenamento em cache e a limitação de taxa da API para manter a compatibilidade e o desempenho em diferentes versões do aplicativo. Melhore a segurança com 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 seus aplicativos principais e permite um melhor desempenho e gerenciamento de recursos. Também ajuda você a aproveitar ao máximo os benefícios da escalabilidade, flexibilidade e eficiência de custos.

Ao mergulhar mais fundo 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 seus aplicativos nativos da nuvem. Essa busca facilita a adoção de padrões de aplicativos 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.

Use tecnologias de service mesh

À medida que as organizações adotam cada vez mais uma arquitetura de microsserviços para criar e implantar aplicativos, o gerenciamento da complexidade, da segurança e das comunicações entre esses serviços se torna essencial. 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.

Garanta visibilidade e rastreabilidade

As práticas modernas oferecem maior visibilidade e rastreabilidade no processo de desenvolvimento e facilitam a conformidade com os padrões e as melhores práticas do setor. Visibilidade e monitoramento são essenciais para o desenvolvimento moderno de aplicativos. A implementação de soluções de monitoramento e registro para fornecer informações valiosas sobre o desempenho dos aplicativos permite que as organizações identifiquem áreas de melhoria e otimizem seus aplicativos. Recomendamos que você trabalhe com suas equipes de engenharia de plataforma para garantir que as ferramentas estejam disponíveis para fornecer end-to-end visibilidade e monitoramento de erros, desempenho e conformidade do aplicativo, para que você possa detectar, diagnosticar e resolver problemas rapidamente.

Excel

Adote microsserviços

Para muitas organizações, o desenvolvimento moderno de aplicativos é sinônimo de sucesso nos negócios. Os microsserviços estão no centro dessa transformação, e as organizações podem se beneficiar da adoção desses poderosos padrões arquitetônicos.

Os microsserviços oferecem uma arquitetura de aplicativos altamente escalável, resiliente e ágil. Ao dividir um aplicativo em serviços pequenos e implantáveis de forma independente, as organizações podem optar por iterar rapidamente em componentes específicos sem afetar outras partes do aplicativo. 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 insalubre, 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 o desempenho ideal.

Outro aspecto crítico da implementação de microsserviços é a adoção dos princípios de design orientado por 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 o aplicativo evolua de acordo com as necessidades da organização.

Otimizar a comunicação entre serviços também é vital em um aplicativo baseado 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 o desempenho geral e a capacidade de manutenção do aplicativo.

Uma organização que adota microsserviços fornece um ambiente que promove inovação, agilidade e colaboração. As equipes de desenvolvimento geralmente são organizadas em torno das capacidades de negócios e têm um forte foco nas práticas de integração contínua e entrega contínua (CI/CD). Eles têm o poder 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 aplicativos e serviços com mais rapidez do que organizações que usam processos tradicionais de desenvolvimento de software e gerenciamento de infraestrutura.

A adoção de DevOpspráticas com integração e entrega contínuas (CI/CD) promotes a streamlined, automated, and efficient process for building, testing, and deploying applications. CI/CDpermite a entrega rápida de software, reduz o risco de erros de implantação e garante que os aplicativos estejam sempre atualizados com os recursos e correções de erros mais recentes). O objetivo principal é evoluir e melhorar aplicativos e serviços em um ritmo mais rápido, evoluindo a partir do uso de processos tradicionais de desenvolvimento de software e gerenciamento de infraestrutura.

Início

Adote 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, estruturas, 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.

Crie pipelines de CI/CD

CI/CD pipelines are sets of automated instructions that are initiated by changes committed to the version control system. They typically include instructions for building the application, running automated tests, and deploying code to a specific environment. You can set up an automated CI/CDfunda usando ferramentas como AWS CodePipelineJenkins ou GitLab CircleCI. Você também pode configurá-los diretamente em sistemas de controle de versão que suportam 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 estágios. 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 ou antes dos feriados. Considere definir regras sobre a implantação de código quando o autor do commit 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.

Implemente testes automatizados

As práticas modernas recomendam mudar para a esquerda (aproximar os testes do desenvolvedor e do IDE e no início do ciclo de vida) para detectar e corrigir problemas antes que eles sejam confirmados em um repositório e iniciem um pipeline. Essa prática envolve ciclos rápidos de feedback com o desenvolvedor, porque os erros são detectados enquanto o desenvolvedor está codificando. Mudar para a esquerda 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.

O teste automatizado detecta erros no início do processo de desenvolvimento e inclui testes unitários, 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 desempenho e testes de aplicativos de segurança.

Crie documentação

Além de implementar um CI/CD pipeline to streamline development workflows, you should maintain clear and comprehensive documentation to ensure the pipeline's ongoing effectiveness, maintainability, and scalability. Documentation is a vital aspect of CI/CD pipeline, porque 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 vantagens 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.

Use a infraestrutura como código

Use ferramentas como Terraform, Ansible ou AWS CloudFormationpara 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 higienizados. Quando possível, faça as alterações e acompanhe essas alterações no código.

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

- Use o controle de versão.
- Faça uso de sistemas de rastreamento de bugs e emissão de bilhetes.
- Peça aos colegas que revisem as alterações antes de aplicá-las.
- Estabeleça padrões e projetos de código de infraestrutura.
- Teste as mudanças na infraestrutura.

Mantenha e acompanhe métricas padrão

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

- Frequência de construção. O número de construções oferece informações sobre a produtividade da sua equipe e a complexidade das mudanças.
- Frequência de implantação. Implantações regulares indicam um processo de desenvolvimento ágil e saudável.
- Prazo de entrega para mudanças. Medir o tempo médio para que as mudanças cheguem à produção pode ajudá-lo a identificar gargalos em seu processo de implantação.
- Tempo médio de passagem pelo pipeline. O tempo médio do estágio inicial do pipeline até cada estágio subsequente pode ajudar a otimizar seu fluxo de trabalho.
- Volume de mudança de produção. Acompanhar o número de mudanças que chegam à produção pode fornecer informações sobre a estabilidade do seu ambiente de produção.

- Tempo de construção. O tempo médio de construção pode indicar possíveis problemas na base de código ou na infraestrutura.

Avançar

Use o gerenciamento de configuração

As ferramentas de gerenciamento de configuração desempenham um papel fundamental na automação da implantação, configuração e gerenciamento de software e infraestrutura. Eles 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.AWS Systems Manager O State Manager é um serviço de gerenciamento de configuração seguro e escalável que automatiza o processo de manter seus nós gerenciados e outros AWS recursos em um estado definido por você.

Integre monitoramento e registro

A integração de soluções de monitoramento e registro 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 informações em tempo real sobre o desempenho do aplicativo, permitir a identificação e a resolução mais rápidas de problemas e promover a melhoria contínua para ajudar a garantir que os aplicativos permaneçam confiáveis, com desempenho e escaláveis durante todo o ciclo de vida. Investir em soluções de monitoramento e registro 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.

Crie uma cadência para mesclagem

Confirme ou mescle alterações de código na ramificação da linha principal (tronco ou principal) pelo menos uma vez por dia ou, idealmente, 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 escuro e técnicas semelhantes para personalizar os recursos que seus clientes usam.

Capture 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 melhores práticas pós-implantação incluem observar os indicadores-chave de desempenho mais importantes (KPIs) e validar se não há erros no ambiente de produção. Automatize o tratamento de erros e a avaliação pós-implantação KPIs 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 o Painel de DevOps monitoramento da solução em AWS.

Excel

Adote práticas e tecnologias de ponta para um desempenho ideal. O refinamento contínuo de seus processos de CI/CD ajuda você a melhorar a qualidade do software, reduzir o tempo de lançamento no mercado e 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 seu aplicativo, configuração, infraestrutura, dados, AWS contas e organizações, pipelines de implantação, redes e controles de segurança e conformidade.
- Crie pipelines de implantação correspondentes para imagens computacionais, serviços compartilhados e aplicativos.
- Considere um GitOps modelo no qual 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 aprendizado de máquina (ML), dados, Internet das Coisas (IoT) e outras cargas de trabalho.
- Assine digitalmente todos os artefatos de construção 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 aplicativos e serviços que automatizaram todo o processo de entrega de software, considere a implantação contínua, na qual 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 AWS site.

Integre tecnologias de IA/ML

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

- Geração automatizada de testes
- Priorização inteligente de testes
- Análise preditiva 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 AWS site.

Adote 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 seu aplicativo 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 o desempenho do seu aplicativo continuamente usando ferramentas de criação de perfil, monitoramento em tempo real e ciclos de feedback. Aplique técnicas como as seguintes para garantir que seus aplicativos 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
- Teste de escalabilidade e desempenho

Implemente observabilidade avançada

Elevar a observabilidade da sua infraestrutura de nuvem vai além do básico de coletar, agregar e analisar métricas, registros e rastreamentos. Quando a observabilidade é aprimorada com ferramentas como a 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 seus aplicativos e infraestrutura, mas também sobre o desempenho e a integridade de todo o sistema, incluindo o próprio pipeline. Esses insights ajudam você a:

- Identifique, compreenda e resolva rapidamente possíveis problemas para melhorar a estabilidade do aplicativo e reduzir o tempo de inatividade
- Simplifique seus processos de CI/CD para criar entregas mais rápidas e confiáveis
- Obtenha insights mais profundos sobre o impacto das mudanças e implantações de código para impulsionar a tomada de decisões informada
- Otimize 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 seus aplicativos e infraestrutura para criar uma visão abrangente do desempenho, comportamento e integridade de seus sistemas.
- Centralize a coleta, o armazenamento e a análise de dados com ferramentas como CloudWatch a Amazon para unificar seus dados de observabilidade e facilitar o acesso e a interpretação.
- Use AWS X-Ray para rastreamento distribuído para entender o desempenho de seus aplicativos e seus serviços subjacentes.
- Estabeleça ciclos 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.

Implemente GitOps práticas

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

Conclusão

Este guia serve como um manual para a implementação e o gerenciamento bem-sucedidos de uma base para a adoção bem-sucedida da nuvem. Ele discute como:

- Aborde 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.
- Desenvolva a engenharia de plataforma com forte provisionamento e orquestração.
- Permita o uso de um ambiente de nuvem compatível com várias contas que gerencia e distribui produtos de nuvem aprovados aos usuários de maneira escalável e repetível.
- Support as decisões de arquitetura de dados com as ferramentas necessárias para que a engenharia de dados conduza a tomada de decisões baseada em dados.
- Combine esses recursos com estratégias modernas de desenvolvimento de aplicativos e processos de CI/CD para promover agilidade, eficiência e inovação em sua organização.
- Crie relacionamentos interfuncionais e receba 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

AWS Recursos do 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 governo
- Perspectiva de operações
- Perspectiva de segurança

Recursos adicionais:

- AWS Centro de Arquitetura
- AWS estudos de caso
- AWS Referência geral
- Glossário da AWS
- AWS Centro de conhecimento
- AWS Orientação prescritiva
- AWS Partner Solutions (anteriormente Quick Starts)
- AWS documentação de segurança
- AWS Biblioteca de soluções
- AWS Treinamento e certificação
- AWS Well-Architected
- AWS whitepapers e guias
- Começando com 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 sênior de soluções, AWS
- Michael Rhyndress, consultor sênior DevSecOps , AWS
- Alex Livingstone, arquiteto principal de soluções e especialista, CloudOps AWS
- Bruce Cooper, diretor da SDE, AWS
- Ravinder Thota, consultor consultivo sênior, AWS
- Sausan Yazji, gerente sênior de prática, AWS
- Paul Duvall, diretor, DevSecOps AWS
- Jeremy Tennant, gerente principal de entrega em nuvem, AWS
- Sneh Shah, líder principal de infraestrutura, AWS
- Sasa Baskarada, líder mundial de estrutura de adoção da AWS nuvem, 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: migre seu banco de dados Oracle local para a edição compatível com o Amazon Aurora PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para o. AWS
- 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 atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja a inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Zona de disponibilidade

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

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

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS

Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

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

acesso em vidro quebrado

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implementar procedimentos de quebra de vidro na orientação do Well-Architected AWS .

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

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

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

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

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

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

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para o Nuvem AWS:

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

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

informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. CI/CD 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.

malha de dados

Uma estrutura arquitetônica que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados que oferece suporte à inteligência comercial, como análises. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja a linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte O que é intercâmbio eletrônico de dados.

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

ambiente

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

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um 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 o planejamento de recursos corporativos.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

transformação de recursos

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

solicitação rápida

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

FGAC

Veja o controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja o modelo da fundação.

modelo de fundação (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

imagem dourada

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais ()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, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

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

o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

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

modernização de historiador

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

dados de retenção

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de aprendizado de máquina. Você pode usar dados de retenção para avaliar o desempenho do modelo comparando as previsões do modelo com os dados de retenção.

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

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

eu

IaC

Veja a infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis. Para obter mais informações, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

VPC de entrada (admissão)

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

migração incremental

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

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das Coisas (IoT)

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

interpretabilidade

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

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

modelo de linguagem grande (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

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 um modelo de linguagem grande.

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

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

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

ramificação principal

Veja a filial.

malware

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

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

conta de membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

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

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

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja o aprendizado de máquina.

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte Estratégia para modernizar aplicativos no Nuvem AWS.

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliação da prontidão para modernização de aplicativos no. Nuvem AWS

aplicações monolíticas (monólitos)

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

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

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

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

Comunicação de processo aberto — Arquitetura unificada (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets

S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

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

ORR

Veja a análise de prontidão operacional.

OT

Veja a tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja as informações de identificação pessoal.

manual

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

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um 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. Para obter mais informações, consulte Habilitar a persistência de dados em microsserviços.

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

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

privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

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

encadeamento imediato

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

pseudonimização

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

publish/subscribe (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um MES baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal no qual outros microsserviços possam se inscrever. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

RAG

Consulte Geração Aumentada de Recuperação.

ransomware

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

Matriz RASCI

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

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

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

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Especificar o que Regiões da AWS sua conta pode usar.

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML 2.0

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte O que há em um segredo do Secrets Manager? na documentação do Secrets Manager.

segurança por design

Uma abordagem de engenharia de sistema 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 principais de controles de segurança: preventivos, detectivos, responsivos e proativos.

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

Uma medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Abordagem em fases para modernizar aplicativos no. Nuvem AWS

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte Estrutura de qualificação AWS da carga de trabalho.

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de dia zero.

vulnerabilidade de dia zero

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

aviso zero-shot

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

eficácia da solicitação zero depende da complexidade da tarefa e da qualidade da solicitação. Veja também a solicitação de algumas fotos.

aplicação zumbi

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

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