AWS Estrutura de migrações seguras: mobilizando segurança e conformidade

AWS Orientação prescritiva

AWS Orientação prescritiva: AWS Estrutura de migrações seguras: mobilizando segurança e conformidade

Table of Contents

Estrutura de migrações seguras da AWS: mobilizando segurança e conformidade

Amazon Web Services (colaboradores)

Março de 2024 (histórico do documento)

As migrações corporativas para a nuvem podem ser complexas, resultando em desafios e riscos se não forem planejadas adequadamente do ponto de vista comercial e técnico. A segurança e a conformidade exigem um planejamento detalhado durante uma jornada de migração e modernização. Muitas organizações percebem a segurança e a conformidade como um obstáculo para a adoção da nuvem. Os diretores de segurança da informação (CISOs) e as equipes de segurança geralmente citam os seguintes desafios comuns ao tomar decisões de adoção da nuvem: incerteza dos recursos de segurança da nuvem, adesão aos requisitos de conformidade, dificuldades no mapeamento da política de segurança, falta de habilidades em segurança na nuvem e baixo apetite ao risco.

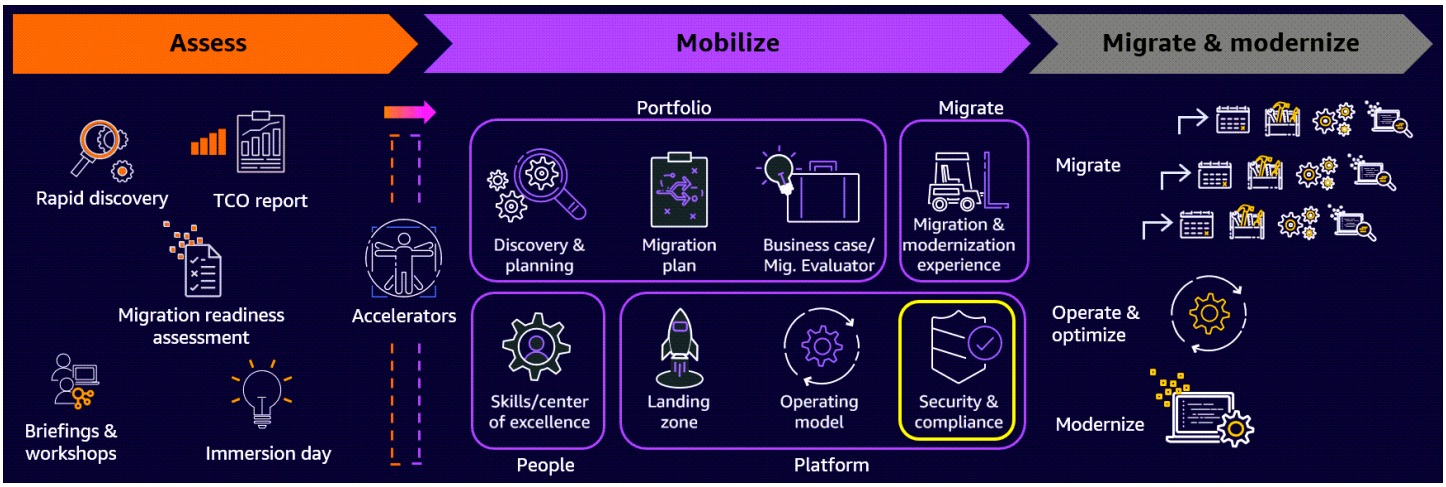
Para enfrentar esses desafios, o AWS Secure Migrations Framework destaca as principais atividades que você deve planejar e gerenciar durante a fase de mobilização de um projeto de migração. Este guia ajuda você a alinhar seus processos, metodologia e abordagem de migração para incluir essas melhores práticas.

Público-alvo

Essa estrutura é destinada para aqueles que estão realizando migrações e modernizações no Nuvem AWS, e também para terceiros que estão apoiando as migrações de seus clientes.

Fluxo de trabalho e estrutura de equipe de segurança e conformidade

AWS oferece o AWS Migration Acceleration Program. Esse programa separa o processo de migração em três fases: avaliar, mobilizar, migrar e modernizar. Como parte da fase de mobilização, você cria um plano de migração e refina seu caso de negócios. Você aborda as lacunas na prontidão da sua organização que foram descobertas na fase de avaliação. Você também se concentra em criar sua landing zone, impulsionar a prontidão operacional e desenvolver habilidades na nuvem. Uma parte fundamental da fase de mobilização é criar um fluxo de trabalho de segurança e conformidade que planeje e atenda aos requisitos de segurança, risco e conformidade para a migração. Conforme mostrado na imagem a seguir, o fluxo de trabalho de segurança e conformidade faz parte da perspectiva de plataforma dessa metodologia de migração.



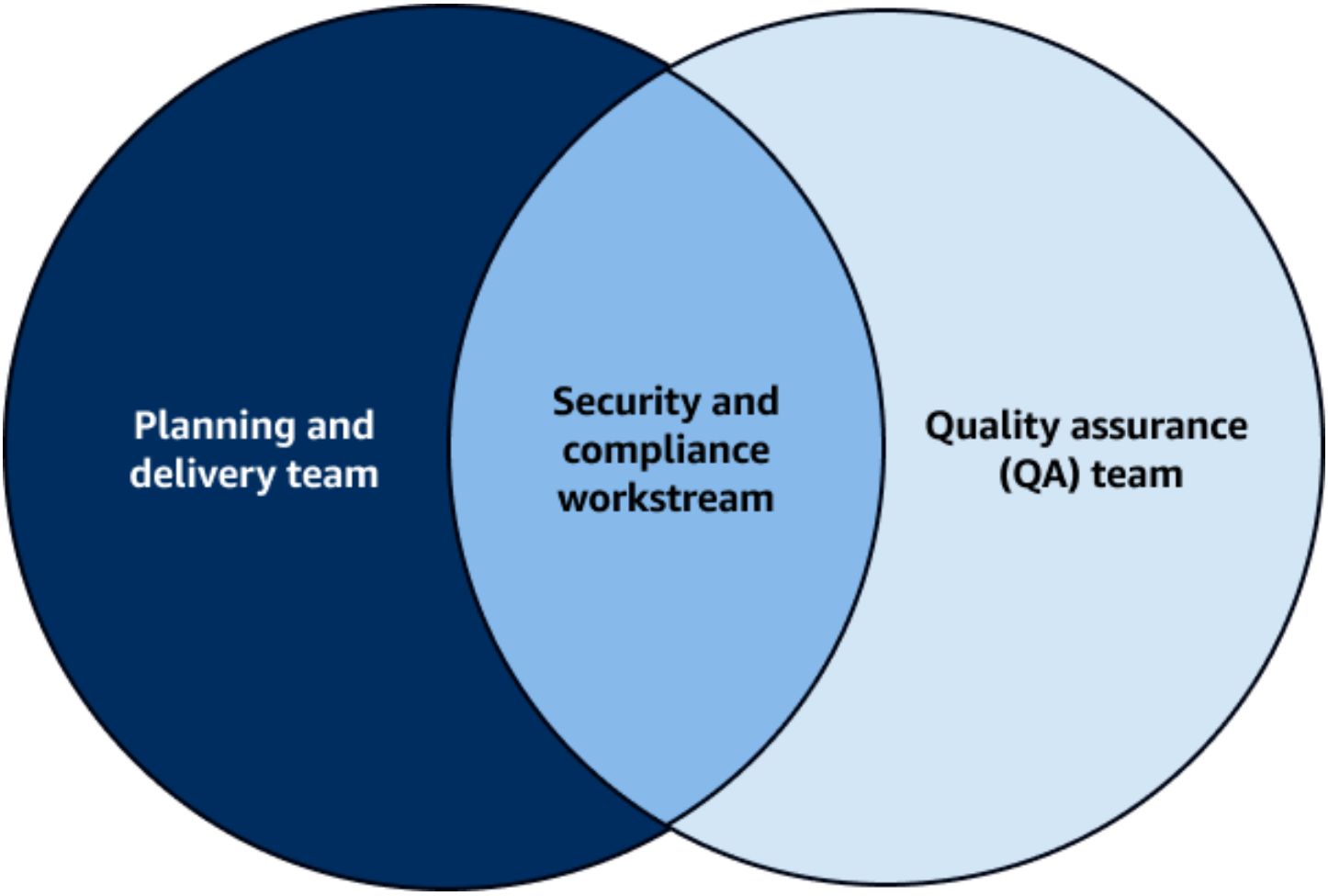
Durante a fase de mobilização, é importante descobrir e planejar seus requisitos de segurança e conformidade. Avalie seus requisitos através das lentes de ferramentas, pessoas e processos. Há cinco domínios principais para o fluxo de trabalho de segurança e conformidade durante a fase de mobilização:

- Descoberta e alinhamento de segurança
- Mapeamento da estrutura de segurança
- Implementação, integração e validação de segurança
- Documentação de segurança
- Operações de nuvem de segurança e conformidade

Essas atividades são discutidas em detalhes no Domínios do fluxo de trabalho de segurança e conformidade capítulo deste guia. Primeiro, é importante entender a composição e a estrutura das equipes que dão suporte ao fluxo de trabalho de segurança e conformidade. Essas equipes realizam ou facilitam as atividades no fluxo de trabalho de segurança e conformidade.

Estrutura da equipe de segurança e conformidade

A primeira etapa para uma mobilização eficaz de segurança e conformidade é configurar ou formar duas equipes que possam apoiar, concluir e governar as cinco principais atividades da estrutura. A imagem a seguir mostra a estrutura de equipe recomendada e os requisitos de recursos. O fluxo de trabalho de segurança e conformidade é composto principalmente por indivíduos da equipe de garantia de qualidade (QA) e da equipe de planejamento e entrega.



A equipe de planejamento e entrega é responsável pelo seguinte no fluxo de trabalho de segurança e conformidade:

- Entendendo o modelo de responsabilidade AWS compartilhada
- Entendendo os serviços de AWS segurança e conformidade no nível 300—400
- Compreendendo o design e a configuração de arquiteturas de conformidade em AWS
- Coletando requisitos de segurança e conformidade usando ferramentas ou mecanismos definidos
- Mapeamento de requisitos de segurança, políticas, configurações, controles e grades de proteção para configurações de serviço em AWS (isso é conhecido como mapeamento da estrutura de segurança)
- Fornecendo pelo menos duas pessoas certificadas em AWS segurança
- Criação de documentação de segurança

A equipe de controle de qualidade é responsável pelo seguinte no fluxo de trabalho de segurança e conformidade:

- Fornecendo um total de 3 a 5 pessoas, e pelo menos duas delas devem ter AWS certificações de segurança
- Compreendendo o design e a configuração da arquitetura de conformidade em AWS
- Compreensão e experiência na conclusão de cinco ou mais avaliações do AWS Well-Architected
- Validar se a AWS infraestrutura e os recursos estão em conformidade com as melhores AWS práticas de segurança e conformidade
- Criação e apresentação de um relatório de validação de segurança

Os requisitos de cada equipe variam de acordo com o tamanho da migração e a complexidade da segurança e da conformidade. Também é importante observar que a estrutura e os requisitos da equipe estão limitados ao seguinte escopo:

- Operação do fluxo de trabalho de segurança e conformidade na fase de mobilização
- Validação de segurança e conformidade da migração e modernização

Após a migração, recomendamos que você estabeleça um Centro de Operações de Segurança (SOC) dedicado para monitorar e governar continuamente a segurança e a conformidade no. Nuvem AWS

Domínios do fluxo de trabalho de segurança e conformidade

Esta seção descreve, em detalhes, os domínios pelos quais o fluxo de trabalho de segurança e conformidade é responsável. Durante a fase de mobilização do seu projeto de migração, esses domínios ajudam a acelerar o planejamento e a implementação de segurança e conformidade em: AWS

- Descoberta e alinhamento de segurança
- Mapeamento da estrutura de segurança
- Implementação, integração e validação de segurança
- Documentação de segurança
- Operações de nuvem de segurança e conformidade

É importante abordar esses domínios durante a fase de mobilização para proteger as atividades de migração durante a fase subsequente de migração e modernização.

Descoberta e alinhamento de segurança

Ao mobilizar um projeto de migração, o primeiro domínio para o fluxo de trabalho de segurança e conformidade é a descoberta e o alinhamento da segurança. Esse domínio tem como objetivo ajudar sua organização a atingir as seguintes metas:

- Treine o fluxo de trabalho de segurança e conformidade sobre os serviços AWS de segurança, os recursos e a adesão à conformidade
- Descubra seus requisitos de segurança e conformidade e as práticas atuais. Considere esses requisitos do ponto de vista da infraestrutura e das operações, incluindo:
  - Desafios e fatores de segurança para o estado final de destino
  - Conjunto de habilidades da equipe de segurança na nuvem
  - Políticas, configurações, controles e barreiras de segurança e conformidade
  - Apetite e linha de base para riscos de segurança
  - Ferramentas de segurança existentes e futuras

Workshops de um dia de imersão

Para se alinhar a essas metas, use dias de imersão em segurança e conformidade. Os dias de imersão são workshops que abrangem uma variedade de tópicos relacionados à segurança, como:

- AWS modelo de responsabilidade compartilhada
- AWS serviços de segurança
- AWS Arquitetura de referência de segurança (AWS SRA)
- AWS conformidade
- Pilar de segurança do AWS Well-Architected Framework

Os workshops do dia de imersão ajudam a estabelecer uma base de conhecimento para sua equipe de segurança. Ele os treina sobre serviços AWS de segurança e melhores práticas de segurança e conformidade. AWS Arquitetos de soluções, serviços AWS profissionais e AWS parceiros podem ajudá-lo a realizar esses workshops interativos. Eles usam apresentações padrão, laboratórios da AWS e atividades de quadro branco para ajudar a preparar suas equipes.

Workshops de descoberta

Após os workshops do dia de imersão, você realiza vários workshops aprofundados sobre segurança e descoberta de conformidade. Isso ajuda suas equipes a descobrir os requisitos atuais de segurança, risco e conformidade (SRC) da infraestrutura, dos aplicativos e das operações. Você analisa esses requisitos por meio das seguintes perspectivas: pessoas, processos e tecnologia. A seguir estão as áreas de descoberta de cada perspectiva.

Perspectiva das pessoas

- Estrutura organizacional — entenda a estrutura e as responsabilidades atuais do fluxo de trabalho de segurança e conformidade.
- Capacidades e conjuntos de habilidades — Tenha conhecimentos práticos e conjuntos de habilidades para Serviços da AWS e para os recursos de segurança e conformidade na nuvem. Isso inclui descoberta, planejamento, implementação e operações.
- Matriz responsável, responsável, consultada, informada (RACI) — Defina as funções e responsabilidades pelas atividades atuais de segurança e conformidade dentro da organização.
- Cultura — Entenda a cultura atual de segurança e conformidade. Priorize a segurança e a conformidade como parte das fases de construção, projeto, implementação e operação. Introduza

as operações de segurança de desenvolvimento (DevSecOps) na cultura de segurança e conformidade da nuvem.

Perspectiva do processo

- Práticas — defina e documente os processos atuais de segurança e conformidade para criar, projetar, implementar e operar. Os processos incluem:
  - Acesso e gerenciamento de identidade
  - Resposta e controles de detecção de incidentes
  - Infraestrutura e segurança de rede
  - Proteção de dados
  - Compliance
  - Continuidade e recuperação dos negócios
- Documentação de implementação — documente políticas de segurança e conformidade, configurações de controle, documentação de ferramentas e documentação de arquitetura. Esses documentos são necessários para cobrir a segurança e a conformidade das áreas de infraestrutura, rede, aplicativos, bancos de dados e implantação.
- Documentação de risco — Crie uma documentação de risco de segurança da informação que descreva o apetite e o limite de risco.
- Validações — Crie requisitos internos e externos de validação e auditoria de segurança.
- Runbooks — Desenvolva runbooks operacionais que cubram os processos atuais e padrão de implementação e governança para segurança e conformidade.

Perspectiva da tecnologia

- Serviços e ferramentas — Use ferramentas para validar sua postura de segurança e conformidade e para impor e governar o cenário atual de TI. Estabeleça ferramentas para as seguintes categorias:
  - Acesso e gerenciamento de identidade
  - Resposta e controles de detecção de incidentes
  - Infraestrutura e segurança de rede
  - Proteção de dados
  - Compliance

- Continuidade e recuperação dos negócios

Durante o workshop AWS de descoberta de segurança, você usa modelos e questionários padronizados de coleta de dados para coletar dados. Em cenários em que você não consegue fornecer as informações devido à falta de clareza dos dados ou dados obsoletos, você pode usar uma ferramenta de descoberta de migração para coletar informações de segurança em nível de aplicativo e infraestrutura. Para obter uma lista das ferramentas de descoberta que você pode usar, consulte Ferramentas de migração de descoberta, planejamento e recomendação na AWS Orientação prescritiva. A lista fornece detalhes sobre os recursos de descoberta e o uso de cada ferramenta. Ele também compara ferramentas para ajudá-lo a escolher a melhor ferramenta para atender aos requisitos e restrições do seu cenário de TI.

Durante a avaliação inicial de segurança, é altamente recomendável que você comece com a modelagem de ameaças. Isso ajuda você a identificar possíveis ameaças e medidas existentes em vigor. Também pode haver requisitos predefinidos e documentados de segurança, conformidade e risco. Para obter mais informações, consulte o workshop sobre modelagem de ameaças para construtores (AWS treinamento) e consulte Como abordar a modelagem de ameaças (postagem AWS no blog). Essa abordagem ajuda você a reconsiderar suas estratégias de segurança e conformidade para implantação, implementação e governança no Nuvem AWS.

Mapeamento da estrutura de segurança

Depois de concluir o domínio de descoberta e alinhamento de segurança, a próxima etapa é concluir o domínio de mapeamento da estrutura de segurança. Esse domínio é um processo de workshop que mapeia os requisitos de segurança e conformidade descobertos para os serviços Nuvem AWS de segurança. Ele também alinha sua arquitetura e suas operações às melhores práticas AWS de segurança e conformidade. O workshop mapeia todos os requisitos do ponto de vista de pessoas, processos e tecnologia para abordar o seguinte:

- AWS infraestrutura
  - Conta da AWS, infraestrutura e proteção de rede
  - Proteção de dados
  - Compliance
  - Detecção e resposta a incidentes
  - Gerenciamento de identidade e acesso

  - Continuidade e recuperação dos negócios
- Aplicação em AWS
  - Seguindo as melhores práticas Serviços da AWS para ajudar a proteger seu aplicativo
  - Controle de acesso para aplicativos, bancos de dados, sistemas operacionais e dados
  - Proteção do sistema operacional
  - Proteção de aplicativos, bancos de dados e dados
  - Detecção e resposta a incidentes
  - Compliance
  - Continuidade e recuperação dos negócios de aplicativos

Ao concluir o domínio de mapeamento da estrutura de segurança, considere o apetite definido pelo risco, a estrutura da equipe, o conjunto de habilidades e capacidades da equipe, os processos de segurança, as políticas de segurança, os controles de segurança, as ferramentas, as operações de segurança e outros requisitos e restrições de segurança. No geral, o mapeamento da estrutura de segurança fornece às organizações uma abordagem sistemática para gerenciar riscos de segurança, manter a conformidade e melhorar continuamente sua postura de segurança, de acordo com os padrões e as melhores práticas do setor.

O processo de mapeamento da estrutura de segurança usa a Arquitetura de Referência de AWS Segurança (AWS SRA), o Pilar de Segurança da AWS Well-Architected Framework, a lente de migração da Well-Architected Framework e o whitepaper AWS Introdução à Segurança. AWS Esses documentos funcionam como referências orientadoras para ajudar você a seguir as AWS melhores práticas de segurança e conformidade na nuvem.

Ao usar modelos de mapeamento padronizados no workshop, você mapeia o requisito para o estado final de destino. Você destaca as ferramentas Serviços da AWS, os processos, as políticas, os controles e as mudanças necessárias para atingir o estado final desejado.

Ao realizar o workshop de mapeamento da estrutura de segurança, você pode usar serviços AWS profissionais, arquitetos de soluções de AWS segurança ou AWS parceiros. Esses recursos podem ajudar você a acelerar e facilitar o workshop. Os workshops de mapeamento da estrutura de segurança podem ser incluídos como parte de uma festa de aceleração baseada na experiência (EBA), liderada por arquitetos de AWS soluções, gerentes de soluções de AWS clientes ou parceiros. AWS A empresa EBA atua como uma aceleradora para ajudar você a criar uma base sólida na Nuvem AWS que siga as melhores práticas de AWS migração e modernização.

Você pode usar o AWS Migration Hub Journeys para planejar, realizar e rastrear migrações para o. AWS AWS Migration Hub Journeys introduz o conceito de uma jornada de migração. AWS Migration Hub Journeys converte uma migração em um pipeline de tarefas relacionadas à migração. Você pode criar uma jornada do zero ou a partir de um dos modelos fornecidos pelo Migration Hub Journeys. Você pode configurar o acesso e convidar colaboradores internos e externos para trabalharem juntos nas migrações. Como resultado, os profissionais de migração podem colaborar, trabalhar em tarefas, realizar migrações e acompanhar o progresso, tudo em um só lugar. AWS Migration Hub O Journeys oferece modelos que abrangem cenários comuns de migração, como migração de rehospedagem (lift and shift), migração para Windows, migração de banco de dados, modernização de mainframe e muito mais.

Implementação, integração e validação de segurança

Depois de mapear seus requisitos de segurança, risco e conformidade, o próximo domínio é a implementação, integração e validação da segurança. Com base nos requisitos identificados, escolha os controles e medidas de segurança apropriados para mitigar os riscos de forma eficaz. Isso pode incluir criptografia, controles de acesso, sistemas de detecção de intrusões ou firewalls. Integre soluções de segurança, como sistemas de detecção e prevenção de intrusões, proteção de terminais e gerenciamento de identidade, à infraestrutura de TI existente para fornecer cobertura de segurança abrangente. Realize avaliações de segurança regulares, incluindo verificação de vulnerabilidades, testes de penetração e análises de código, para validar a eficácia dos controles de segurança e identificar pontos fracos ou lacunas. Ao se concentrar na implementação, integração e validação da segurança, as organizações podem fortalecer sua postura de segurança, reduzir a probabilidade de violações de segurança e demonstrar conformidade com os requisitos regulamentares e os padrões do setor.

Implementação

Primeiro, atualize a documentação de acordo com seu limite ou apetite atual de segurança, risco e conformidade. Isso permite que você implemente os requisitos, controles, políticas e ferramentas planejados de segurança e conformidade na nuvem. Essa etapa é necessária somente se você tiver um registro de risco existente e um apetite definido, o que teria sido identificado durante os workshops de descoberta.

Em seguida, você implementa os requisitos, controles, políticas e ferramentas planejados de segurança e conformidade na nuvem. Recomendamos que você os implemente na seguinte ordem: infraestrutura, sistema operacional e Serviços da AWS, em seguida, aplicativo ou banco de dados.

Use as informações na tabela a seguir para garantir que você tenha abordado todas as áreas necessárias de segurança e conformidade.

Área	Requisitos de segurança e conformidade

Infraestrutura	• Conta da AWS
	• Zona de pouso
	  • Controles preventivos
	  • Controles de detecção
	• Segmentação de rede
	• Controle de acesso
	• Criptografia
	• Registro, monitoramento e alertas

Serviços da AWS	• AWS service (Serviço da AWS) configuração
	• Instâncias
	  • Armazenamento
	  • Rede
	• Controle de acesso
	• Criptografia
	• Atualizações e patches
	• Registro, monitoramento e alertas

Sistema operacional	• Antivírus

	• Proteção contra malware e worm • Configuração • Proteção de rede • Controle de acesso • Criptografia • Atualizações e patches • Registro, monitoramento e alertas
Aplicativo ou banco de dados	• Configuração • Código e esquema • Controle de acesso • Criptografia • Atualizações e patches • Registro, monitoramento e alertas

Integração

A implementação da segurança geralmente requer integração com o seguinte:

- Rede — Rede interna e externa à Nuvem AWS

- Cenário de TI híbrida — ambientes de TI diferentes do Nuvem AWS, como locais, nuvens públicas, nuvens privadas e colocations
- Software ou serviços externos — Software e serviços que são gerenciados por fornecedores independentes de software (ISVs) e não estão hospedados em seu ambiente.
- Serviços de modelo operacional em AWS nuvem — serviços de modelo operacional em nuvem que fornecem DevSecOps recursos.

Durante a fase de avaliação do seu projeto de migração, use ferramentas de descoberta, documentação existente ou workshops de entrevistas com aplicativos para identificar e confirmar esses pontos de integração de segurança. Ao projetar e implementar as cargas de trabalho no Nuvem AWS, estabeleça essas integrações de acordo com as políticas e processos de segurança e conformidade que você definiu durante os workshops de mapeamento.

Validação

Após a implementação e a integração, a próxima atividade é validar a implementação. Você garante que a configuração esteja alinhada às AWS melhores práticas de segurança e conformidade. Recomendamos que você valide a segurança de duas áreas de cobertura:

- Avaliação de vulnerabilidade e teste de penetração específicos da carga de trabalho - Valide a segurança do sistema operacional, do aplicativo, do banco de dados ou da rede das cargas de trabalho executadas. Serviços da AWS Para realizar essas validações, use ferramentas e scripts de teste existentes. É importante cumprir a política de suporte ao cliente do teste de AWS penetração ao realizar essas avaliações.
- AWSvalidação de melhores práticas de segurança - Valide se sua AWS implementação está em conformidade com o AWS Well Architected Framework e outros benchmarks selecionados, como o Center for Internet Security (CIS). Para essa validação, você pode usar ferramentas e serviços como Prowler (GitHub) AWS Trusted Advisor, AWS Service Screener () ou AWS Self-Service Security Assessment (GitHub). GitHub

É importante documentar e comunicar todas as descobertas de segurança e conformidade à equipe de segurança e aos líderes. Padronize os modelos de relatórios e use-os para facilitar a comunicação com a respectiva parte interessada em segurança. Documente todas as exceções feitas durante a busca de remediação e certifique-se de que as respectivas partes interessadas em segurança concordem.

Documentação de segurança

Ao mobilizar a segurança e a conformidade durante uma migração, é essencial definir e documentar como você implementa a segurança e a conformidade na nuvem. A documentação deve incluir o seguinte:

- Documentação de implementação de segurança e conformidade — Crie um ou mais documentos que detalham sua definição, processo, políticas, controles, configurações e ferramentas de segurança e conformidade. Certifique-se de que esses documentos abordem esses aspectos de uma Nuvem AWS perspectiva. Inclua o seguinte nesta documentação:
  - Acesso e gerenciamento de identidade
  - Resposta e controles de detecção de incidentes
  - Infraestrutura e segurança de rede
  - Proteção de dados
  - Compliance
  - Continuidade e recuperação dos negócios
- Runbooks de segurança e conformidade — Crie um caderno operacional de segurança e conformidade que guie a equipe de operações de nuvem. Eles devem detalhar como concluir tarefas, atividades e mudanças de segurança e conformidade na nuvem como parte dos requisitos operacionais. Isso inclui monitoramento de segurança e conformidade, gerenciamento de incidentes, validação e melhoria contínua. Certifique-se de que seus runbooks atendam aos requisitos que você identificou durante a descoberta de segurança e o domínio de alinhamento.
- Matriz RACI de segurança na nuvem — Crie uma matriz responsável, responsável, consultada e informada (RACI) que defina responsabilidades e partes interessadas em segurança e conformidade nas seguintes áreas:
  - Design e desenvolvimento
  - Implantação e implementação
  - Operações

Operações de nuvem de segurança e conformidade

O domínio final são as operações em nuvem de segurança e conformidade. Essa é uma atividade contínua em que você usa os runbooks operacionais de segurança e conformidade definidos para governar as operações na nuvem. Você também cria um modelo operacional de nuvem

de segurança para determinar as responsabilidades pela segurança e conformidade em sua organização.

Modelo operacional de nuvem de segurança e conformidade

Nesse domínio, você define um modelo operacional de nuvem para segurança. Seu modelo operacional de nuvem deve atender aos requisitos que você identificou durante os workshops de descoberta e posteriormente definiu como runbooks. Você pode projetar o modelo operacional de nuvem de segurança e conformidade de uma das três maneiras:

- Centralizado — Um modelo mais tradicional, responsável por identificar e remediar eventos de segurança em toda a empresa. SecOps Isso pode incluir a análise das descobertas gerais sobre a postura de segurança da empresa, como problemas de correção e configuração de segurança.
- Descentralizado — a responsabilidade de responder e remediar eventos de segurança em toda a empresa foi delegada aos proprietários do aplicativo e às unidades de negócios individuais, e não há uma função central de operações. Normalmente, ainda há uma função abrangente de governança de segurança que define políticas e princípios.
- Híbrido — Uma combinação de ambas as abordagens, em que SecOps ainda tem um nível de responsabilidade e propriedade para identificar e orquestrar a resposta aos eventos de segurança, e a responsabilidade pela remediação é de propriedade dos proprietários do aplicativo e das unidades de negócios individuais.

É importante selecionar o modelo operacional certo com base nos requisitos de segurança e conformidade, na maturidade e nas restrições da organização. Os requisitos e restrições de segurança e conformidade foram identificados durante o workshop de descoberta. A maturidade da organização, por outro lado, define o nível das práticas de segurança operacional. Veja a seguir um exemplo de uma faixa de maturidade:

- Baixo — O registro é local e algumas ações ou ações esporádicas são realizadas.
- Intermediário — Os registros de diferentes fontes são correlacionados e o alerta automático é estabelecido.
- Alto — Existem manuais detalhados que contêm detalhes sobre as respostas padronizadas do processo. Operacional e tecnicamente, a maioria das respostas de alerta é automatizada.

Para entender melhor o modelo operacional de segurança e conformidade na nuvem e auxiliar na seleção de um design adequado, consulte Considerações sobre operações de segurança na nuvem

(postagem no AWS blog). Em cenários em que não há requisitos predefinidos, recomendamos que você configure um Centro de Operações de Segurança (SOC) como parte do modelo operacional em nuvem. Normalmente, essa é uma prática de modelo operacional centralizado. Com essa abordagem, você pode direcionar eventos de várias fontes para uma equipe centralizada, que pode então acionar ações e respostas. Isso padroniza a governança da segurança por meio de operações na nuvem. AWS e AWS os parceiros têm a capacidade de ajudá-lo a criar um SOC e definir e implementar a orquestração, automação e resposta de segurança (SOAR). AWS e AWS os parceiros usam consultas de serviços profissionais Serviços da AWS, modelos definidos e ferramentas de terceiros dos AWS parceiros.

Operações de segurança contínuas

Nesse domínio, execute as seguintes tarefas continuamente usando seus runbooks de operações de segurança e conformidade definidos:

- Monitoramento de segurança e conformidade — realize o monitoramento centralizado de eventos e ameaças de segurança usando suas ferramentas Serviços da AWS, métricas, critérios e frequência definidos. A equipe de operações ou o SOC administram esse monitoramento contínuo, dependendo da estrutura da sua organização. O monitoramento de segurança envolve análise e correlação de grandes quantidades de registros e dados. Os dados de log vêm de endpoints, redes Serviços da AWS, infraestrutura e aplicativos e são armazenados em um repositório centralizado, como o Amazon Security Lake ou um sistema de gerenciamento de eventos e informações de segurança (SIEM). É importante configurar alertas para que você possa responder manual ou automaticamente aos eventos em tempo hábil.
- Gerenciamento de incidentes — defina sua postura básica de segurança. Quando ocorrer um desvio de uma linha de base predefinida, seja por configuração incorreta ou por fatores externos, registre um incidente. Certifique-se de que uma equipe designada responda a esses incidentes. A base de um programa bem-sucedido de resposta a incidentes na nuvem é ter pessoas, processos e ferramentas integrados em cada estágio do programa de resposta a incidentes (preparação, operações e atividade pós-incidente). Educação, treinamento e experiência são vitais para um programa bem-sucedido de resposta a incidentes na nuvem. Idealmente, eles são implementados bem antes de ter que lidar com um possível incidente de segurança. Para obter mais informações sobre como configurar um programa eficaz de resposta a incidentes de segurança, consulte o Guia de resposta a incidentes de AWS segurança. Você também pode usar o workshop AWS Incident Manager - Automatize a resposta a incidentes a eventos de segurança para ajudar a documentar e treinar suas equipes sobre o Serviços da AWS que pode melhorar o gerenciamento de incidentes, aumentar a visibilidade e reduzir o tempo de recuperação.

- Validação de segurança — A validação de segurança envolve a execução de avaliação de vulnerabilidade, testes de penetração e testes de eventos simulados de segurança caótica. A validação de segurança deve continuar sendo executada periodicamente, especialmente nos seguintes cenários:
  - Atualizações e lançamentos de software
  - Ameaças recém-identificadas, como malware, vírus ou worms
  - Requisitos de auditoria interna e externa
  - Violações de segurança

  É importante documentar o processo de validação de segurança e destacar as pessoas, o processo, o cronograma, as ferramentas e os modelos para coleta de dados e geração de relatórios. Isso padroniza as validações de segurança. Continue cumprindo a política de suporte AWS ao cliente para testes de penetração ao executar validações de segurança na nuvem.
- Auditorias internas e externas — Conduza auditorias internas e externas para validar se as configurações de segurança e conformidade atendem aos requisitos normativos ou de políticas internas. Realize auditorias periodicamente com base em um cronograma predefinido. As auditorias internas são normalmente conduzidas por uma equipe interna de segurança e risco. As auditorias externas são conduzidas por agências relevantes ou funcionários padrão. Você pode usar Serviços da AWS, como AWS Audit Managere AWS Artifact, para facilitar o processo de auditoria. Esses serviços podem fornecer evidências relevantes para relatórios de auditoria de TI de segurança. Eles também podem simplificar o gerenciamento de riscos e conformidade com os padrões regulatórios e do setor, automatizando a coleta de evidências. Isso ajuda você a avaliar se as políticas, procedimentos e atividades conhecidos como controles estão operando de forma eficaz. Também é importante alinhar os requisitos de auditoria com seus parceiros de serviços gerenciados para garantir a conformidade.

Análise da arquitetura de segurança — conclua uma revisão e atualização periódicas de sua AWS arquitetura do ponto de vista de segurança e conformidade. Revise a arquitetura trimestralmente ou quando houver alterações na arquitetura. AWS continua lançando atualizações e melhorias nos recursos e serviços de segurança e conformidade. Use a Arquitetura AWS de Referência de Segurança e a Ferramenta AWS Well Architected para facilitar essas revisões de arquitetura. É importante documentar sua implementação de segurança e conformidade e as alterações recomendadas após o processo de análise.

AWS serviços de segurança para operações

Você compartilha a responsabilidade AWS pela segurança e conformidade no Nuvem AWS. Esse relacionamento é descrito em detalhes no modelo de responsabilidade AWS compartilhada. Enquanto AWS gerencia a segurança da nuvem, você é responsável pela segurança na nuvem. Você é responsável por proteger seu próprio conteúdo, infraestrutura, aplicativos, sistemas e redes, da mesma forma que faria com um data center local. Suas responsabilidades pela segurança e conformidade Nuvem AWS variam de acordo com os serviços que você usa, como você integra esses serviços ao seu ambiente de TI e as leis e regulamentações aplicáveis.

Uma vantagem disso Nuvem AWS é que ele permite que você escale e inove usando as AWS melhores práticas e serviços de segurança e conformidade. Isso ajuda você a manter um ambiente seguro pagando somente pelos serviços que você usa. Você também tem acesso aos mesmos serviços de AWS segurança e conformidade que as organizações corporativas altamente protegidas usam para proteger seus ambientes de nuvem.

Construir uma arquitetura de nuvem em uma base sólida e segura é a primeira e a melhor etapa para garantir a segurança e a conformidade da nuvem. No entanto, seus AWS recursos são tão seguros quanto você os configura. Uma postura eficaz de segurança e conformidade é alcançada somente por meio da adesão contínua e estrita em um nível operacional. As operações de segurança e conformidade podem ser amplamente agrupadas em cinco categorias:

- Proteção de dados
- Acesso e gerenciamento de identidade
- Proteção de rede e aplicativos
- Detecção de ameaças e monitoramento contínuo
- Conformidade e privacidade de dados

AWS os serviços de segurança e conformidade são mapeados para essas categorias para ajudá-lo a atender a um conjunto abrangente de requisitos. Agrupados nessas categorias, a seguir estão os principais serviços AWS de segurança e conformidade e seus recursos. Esses serviços podem ajudar você a criar e aplicar a governança da segurança na nuvem.

Proteção de dados

AWS fornece os seguintes serviços que podem ajudá-lo a proteger seus dados, contas e cargas de trabalho contra acesso não autorizado:

- AWS Certificate Manager— Provisione, gerencie e implante certificados SSL/TLS para uso com. Serviços da AWS
- AWS CloudHSM— Gerencie seus módulos de segurança de hardware (HSMs) no Nuvem AWS.
- AWS Key Management Service (AWS KMS) — Crie e controle as chaves usadas para criptografar seus dados.
- Amazon Macie — Descubra, classifique e ajude a proteger dados confidenciais com recursos de segurança baseados em aprendizado de máquina.
- AWS Secrets Manager— alterne, gerencie e recupere credenciais de banco de dados, chaves de API e outros segredos ao longo de seu ciclo de vida.

Gerenciamento de identidade e acesso

Os serviços de AWS identidade a seguir ajudam você a gerenciar com segurança identidades, recursos e permissões em grande escala:

- Amazon Cognito — Adicione cadastro, login e controle de acesso de usuários aos seus aplicativos web e móveis.
- AWS Directory Service— Use o Microsoft Active Directory gerenciado no Nuvem AWS.
- AWS IAM Identity Center— gerencie centralmente o acesso de login único (SSO) a vários Contas da AWS aplicativos comerciais.
- AWS Identity and Access Management (IAM) — Controle com segurança o acesso Serviços da AWS e os recursos.
- AWS Organizations— implemente o gerenciamento baseado em políticas para vários. Contas da AWS
- AWS Resource Access Manager (AWS RAM) — Compartilhe AWS recursos em suas contas.

Proteção de rede e aplicativos

Essa categoria de serviços ajuda você a aplicar uma política de segurança refinada em pontos de controle de rede em toda a organização. O seguinte Serviços da AWS ajuda você a inspecionar e filtrar o tráfego para ajudar a impedir o acesso não autorizado a recursos nos limites do host, da rede e do aplicativo:

- AWS Firewall Manager— configure e gerencie AWS WAF regras Contas da AWS e aplicativos em um local central.

- AWS Network Firewall— Implemente proteções de rede essenciais para suas nuvens privadas virtuais (VPCs).
- Firewall de DNS do Amazon Route 53 Resolver — Ajude a proteger suas solicitações de DNS de saída do seu. VPCs
- AWS Shield— Proteja seus aplicativos da web com a proteção DDo S gerenciada.
- AWS Systems Manager— Configure e gerencie o Amazon Elastic Compute Cloud (Amazon EC2) e sistemas locais para aplicar patches de sistema operacional, criar imagens seguras do sistema e configurar sistemas operacionais.
- Amazon Virtual Private Cloud (Amazon VPC) — Provisione uma seção logicamente isolada de AWS onde você pode lançar AWS recursos em uma rede virtual que você define.
- AWS WAF— Ajude a proteger seus aplicativos da Web contra explorações comuns da Web.

Detecção de ameaças e monitoramento contínuo

Os seguintes serviços de AWS monitoramento e detecção ajudam você a identificar possíveis incidentes de segurança em seu AWS ambiente:

- AWS CloudTrail— Rastreie a atividade do usuário e o uso da API para permitir a governança e a auditoria operacional e de risco do seu Conta da AWS.
- AWS Config— registre e avalie as configurações de seus AWS recursos para ajudá-lo a auditar a conformidade, rastrear alterações nos recursos e analisar a segurança dos recursos.
- AWS Config regras — crie regras que atuem automaticamente em resposta às mudanças em seu ambiente, como isolar recursos, enriquecer eventos com dados adicionais ou restaurar uma configuração para um estado em boas condições.
- Amazon Detective — Analise e visualize dados de segurança para chegar rapidamente à causa raiz de possíveis problemas de segurança.
- Amazon GuardDuty — Ajude a proteger suas Contas da AWS cargas de trabalho com detecção inteligente de ameaças e monitoramento contínuo.
- Amazon Inspector — Automatize as avaliações de segurança para ajudar a melhorar a segurança e a conformidade de seus aplicativos que são implantados em. AWS
- AWS Lambda— Execute código sem provisionar ou gerenciar servidores para que você possa escalar sua resposta programada e automatizada a incidentes.
- AWS Security Hub— Visualize e gerencie alertas de segurança e automatize as verificações de conformidade a partir de um local central.

Conformidade e privacidade de dados

O seguinte Serviços da AWS fornece uma visão abrangente do seu status de conformidade. Eles monitoram continuamente seu ambiente usando verificações automatizadas de conformidade baseadas nas AWS melhores práticas e nos padrões do setor:

- AWS Artifact— Obtenha acesso sob demanda a relatórios AWS de segurança e conformidade e selecione contratos on-line.
- AWS Audit Manager— audite continuamente seu AWS uso para simplificar a forma como você gerencia os riscos e mantém a conformidade com as regulamentações e os padrões do setor.

Conclusão

A segurança e a conformidade da nuvem são essenciais para o sucesso e o crescimento da jornada de adoção da nuvem de uma organização. Os requisitos de segurança e conformidade devem ser reunidos e analisados. Do ponto de vista da prontidão para a nuvem, é fundamental identificar as lacunas no início de sua jornada de migração. A fase de mobilização do AWS Migration Acceleration Program recomenda que você crie um fluxo de trabalho de segurança e conformidade para essa finalidade. Quando esse fluxo de trabalho funciona de forma eficaz, ele cria uma base de nuvem sólida e segura para uma jornada bem-sucedida de migração e modernização da nuvem. Recomendamos que você consulte e incorpore a abordagem e os processos detalhados nessa estrutura em sua prática de migração e modernização para planejar e implementar adequadamente as bases seguras da nuvem.

Recursos

AWS documentação

- AWS Guia de resposta a incidentes de segurança (AWS white paper)
- AWS Arquitetura de referência de segurança (AWS SRA) (orientação AWS prescritiva)
- Introdução à AWS segurança (AWS whitepaper)
- Lente de migração (AWS Well-Architected Framework)
- Mobilize sua organização para acelerar migrações em grande escala (AWS orientação prescritiva)
- Pilar de segurança (AWS Well-Architected Framework)

Outros AWS recursos

- AWS Política de Suporte ao Cliente para Testes de Penetração
- AWS Gerenciador de incidentes - Automatize a resposta a incidentes a eventos de segurança (AWS workshop)
- AWS Modelo de responsabilidade compartilhada
- Considerações sobre operações de segurança na nuvem (postagem no AWS blog)

Colaboradores

Autoria

- Ahilan Thiagarajah, principal arquiteto de soluções de parceiros, AWS
- Rishi Singla, arquiteto sênior de soluções de parceiros, AWS
- Venkatesh Krishnan, arquiteto sênior de soluções de parceiros, AWS

Analisando

- Magesh Dhanasekaran, arquiteto de segurança, AWS
- Wana Tun, arquiteta sênior de soluções, AWS

Redação técnica

- Lilly AbouHarb, redatora técnica sênior, AWS

Histórico do documento

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

Alteração	Descrição	Data
Publicação inicial	—	11 de março de 2024

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

- Refatorar/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 das aplicações conectadas enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

função agregada

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

AI

Veja a inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para 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 is commonly described as a pipeline. CI/CDpode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

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

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja a linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

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

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja o planejamento de recursos corporativos.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

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

transformação de recursos

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

solicitação rápida

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

FGAC

Veja o controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja o modelo da fundação.

modelo de fundação (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

imagem dourada

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais ()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 típico de uma DevOps versão.

período de hipercuidados

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

eu

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

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 sistemas que leva em conta a segurança em todo o processo de desenvolvimento.

controle de segurança

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

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

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

CUSPE

Veja um único ponto de falha.

esquema de estrelas

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores

para armazenar atributos de dados. Essa estrutura foi projetada para uso em um data warehouse ou para fins de inteligência comercial.

padrão strangler fig

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

sub-rede

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

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A

ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte Estrutura de qualificação AWS da carga de trabalho.

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

aviso zero-shot

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

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

aplicação zumbi

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

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