Adoção da Zero Trust: uma estratégia para transformação empresarial segura e ágil

AWS Orientação prescritiva

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

AWS Orientação prescritiva: Adoção da Zero Trust: uma estratégia para transformação empresarial segura e ágil

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

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

Table of Contents

Introdução 1
Processos de tomada de decisão 1
Resultados de negócios desejados 4
Postura de segurança aprimorada. 4
Adoção perfeita da nuvem 4
Conformidade e alinhamento regulatório 4
Proteção de dados aprimorada 5
Resposta eficiente a incidentes 5
Maior produtividade da força de trabalho 6
Ativar a transformação digital 6
Resumo da seção 7
Princípios Zero Trust 8
Verificar e autenticar 8
Acesso de privilégio mínimo 8
Microssegmentação 8
Monitoramento e análise contínuos 9
Automação e orquestração 9
Autorização 9
Resumo da seção 10
Principais componentes da ZTA 11
Gerenciamento de identidade e acesso 11
Secure Access Service Edge 11
Prevenção de perda de dados 11
Gerenciamento de eventos e informações de segurança 12
Catálogo de propriedade de recursos corporativos 12
Gerenciamento de endpoints unificados 12
Pontos de fiscalização baseados em políticas 13
Resumo da seção 13
Prontidão organizacional 14
Alinhamento e comunicação da liderança 14
Desenvolvimento e treinamento de habilidades 15
Estrutura organizacional e funções 15
Infraestrutura e arquitetura de TI 16
Gerenciamento de riscos, governança e controle de alterações 16

Monitoramento e avaliação ... 17
Resumo da seção ... 17
Mentalidade de confiança zero ... 19
Educação e treinamento Zero Trust ... 19
Colaboração e comunicação ... 19
Aprendizado e melhoria contínuos ... 19
Métricas e responsabilidade ... 19
Resumo da seção ... 20
Abordagem em fases ... 21
Fase 1: avaliação e planejamento ... 21
Fase 2: condução e implementação ... 22
Fase 3: monitoramento e melhoria contínua ... 22
Resumo da seção ... 23
Práticas recomendadas ... 24
Principais conclusões ... 28
Próximas etapas ... 30
Perguntas frequentes ... 31
O que é Zero Trust? ... 31
O que Serviços da AWS pode me ajudar a implementar a arquitetura de confiança zero? ... 31
Como posso garantir a segurança de dados com a AWS? ... 31
Pode AWS ajudar com os requisitos de conformidade em um ambiente Zero Trust? ... 31
Existem AWS ferramentas ou serviços para automatizar a segurança em um ambiente Zero Trust? ... 32
Como posso garantir o monitoramento contínuo e a resposta a incidentes em um ambiente de nuvem Zero Trust com AWS ... 32
Recursos ... 33
Referências ... 33
Ferramentas ... 33
Histórico do documento ... 35
Glossário ... 36
... 36
A ... 37
B ... 40
C ... 42
D ... 45
E ... 50

F 52
G 54
H 55
eu 56
L 59
M 60
O 64
P 67
Q 70
R 70
S 74
T 78
U 79
V 80
W 80
Z 81
..... lxxxiii

Adoção da Zero Trust: uma estratégia para transformação empresarial segura e ágil

Greg Gooden, Amazon Web Services (AWS)

Dezembro de 2023 (histórico do documento)

Hoje, mais do que nunca, as organizações estão se concentrando na segurança como prioridade fundamental. Isso permite uma ampla gama de benefícios, desde manter a confiança de seus clientes até melhorar a mobilidade da sua força de trabalho e liberar novas oportunidades de negócios digitais. Enquanto fazem isso, a pergunta antiga continua: quais são os padrões ideais para garantir os níveis corretos de segurança e disponibilidade para meus sistemas e dados? Cada vez mais, a Zero Trust se tornou o termo usado para descrever a resposta moderna a essa pergunta.

A arquitetura de confiança zero (ZTA) é um modelo conceitual e um conjunto associado de mecanismos cujo foco é fornecer controles de segurança aos ativos digitais que não dependem única ou fundamentalmente dos tradicionais controles ou perímetros de rede. Em vez disso, os controles de rede são aumentados com identidade, dispositivo, comportamento e outros contextos e sinais ricos para tomar decisões de acesso mais granulares, inteligentes, adaptáveis e contínuas. Ao implementar um modelo ZTA, você pode alcançar uma próxima iteração significativa na maturação contínua da segurança cibernética e dos conceitos de defesa em profundidade, particularmente.

Processos de tomada de decisão

A implementação de uma estratégia de ZTA requer planejamento e tomada de decisão cuidadosos. Envolve avaliar diversos fatores e alinhá-los às metas organizacionais. Os principais processos de tomada de decisão para embarcar em uma jornada com a ZTA incluem:

1. Engajamento das partes interessadas — É crucial envolver outros CxOs gerentes e gerentes seniores para entender suas prioridades, preocupações e visão sobre a postura de segurança de sua organização. VPs Ao envolver os principais investidores desde o início, você pode alinhar a implementação da ZTA com os objetivos estratégicos gerais e obter o suporte e os recursos necessários.
2. Avaliação de risco: a realização de uma avaliação de risco abrangente ajuda a identificar problemas, área de superfície excessiva e ativos críticos, o que ajuda você a tomar decisões informadas sobre controles de segurança e investimento. Avalie a postura de segurança existente

na sua organização, identifique possíveis pontos fracos e priorize as áreas de melhoria com base no cenário de risco específico do seu setor e ambiente operacional.

3. Avaliação de tecnologia: o trabalho de avaliar o cenário tecnológico existente na organização e identificar lacunas ajuda na seleção de ferramentas e soluções apropriadas que se alinhem aos princípios da ZTA. Essa avaliação deve incluir uma análise completa de:
   - Arquitetura de rede
   - Sistemas de gerenciamento de identidade e acesso
   - Mecanismos de autenticação e autorização
   - Gerenciamento de endpoints unificados
   - Ferramentas e processos de propriedade de recursos
   - Tecnologias de criptografia
   - Recursos de monitoramento e registro em log
   - A escolha da pilha de tecnologia certa é crucial para criar um modelo de ZTA robusto.
4. Gerenciamento de alterações: é essencial reconhecer os impactos culturais e organizacionais da adoção de um modelo de ZTA. A implementação de práticas de gerenciamento de alterações ajuda a garantir transição perfeita e aceitação em toda a organização. Envolve educar os funcionários sobre os princípios e benefícios da ZTA, fornecer treinamento sobre novas práticas de segurança e promover uma cultura preocupada com a segurança que incentive a responsabilidade e o aprendizado contínuo.

Esta orientação prescritiva visa fornecer CxOs aos gerentes seniores uma estratégia abrangente para a implementação do ZTA. VPs Ela se aprofundará nos principais aspectos da ZTA, o que inclui:

- Prontidão organizacional
- Abordagens de adoção em fases
- Colaboração dos investidores
- Práticas recomendadas para obter uma transformação empresarial segura e ágil

Seguindo essa orientação, sua organização pode navegar pelo cenário da ZTA e alcançar resultados bem-sucedidos em sua jornada de segurança na nuvem da Amazon Web Services (AWS). AWS oferece uma variedade de serviços que você pode usar para implementar um ZTA, como AWS Identity and Access Management (IAM) Acesso Verificado pela AWS, Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway e

Amazon. GuardDuty Esses serviços podem ajudar a proteger AWS os recursos contra acesso não autorizado.

Resultados de negócios desejados

Esta seção discute os resultados esperados associados à definição e à implementação de uma arquitetura de confiança zero na sua organização.

Postura de segurança aprimorada.

Ao adotar os princípios Zero Trust, uma organização pode fortalecer sua postura de segurança, diminuir os riscos de segurança e proteger a infraestrutura e os dados na nuvem. O princípio fundamental do Zero Trust de conceder acesso em uma need-to-know base, juntamente com controles rigorosos, reduz significativamente a área de superfície e limita o impacto potencial dos eventos de segurança. Essa abordagem proativa ajuda as organizações a se anteciparem aos riscos de segurança emergentes e ajuda a garantir a confidencialidade, integridade e disponibilidade dos ativos.

Adoção perfeita da nuvem

O desenvolvimento de um plano bem definido de adoção da arquitetura de confiança zero (ZTA) pode ajudar a garantir uma transição tranquila e bem-sucedida para o ambiente de nuvem. Os princípios da ZTA se alinham estreitamente às práticas recomendadas de segurança na nuvem, fornecendo uma base sólida para que as organizações obtenham com segurança os benefícios da computação em nuvem. A incorporação dos princípios da ZTA desde o início ajuda sua organização a projetar a arquitetura da nuvem com a segurança como elemento central.

Conformidade e alinhamento regulatório

A implementação das práticas da ZTA pode ajudar sua organização a atender aos requisitos e padrões regulatórios e do setor. A ZTA promove inerentemente o princípio do privilégio mínimo e impõe controles de acesso rígidos. Os controles de acesso geralmente são exigidos por regulamentações como as seguintes:

- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS).

Ao adotar a Zero Trust, uma organização pode ajudar a demonstrar seu compromisso com a proteção de dados, a privacidade e a conformidade regulatória, minimizando a possibilidade de penalizações ou danos à reputação.

Proteção de dados aprimorada

As organizações podem proteger dados confidenciais em todo o processo de adoção da nuvem implementando criptografia de dados, controles de acesso e avaliações regulares de segurança. Sua organização pode executar as seguintes etapas específicas:

- Criptografia de dados: é o processo de criptografar dados de texto não criptografado em texto cifrado de uma forma que uma chave seja exigida para descriptografar os dados de volta ao formato original. Isso torna muito mais difícil para pessoas não autorizadas acessarem dados confidenciais, mesmo que consigam obter uma cópia dos dados.
- Controles de acesso: restringem quem pode acessar dados confidenciais e o que podem fazer com eles. Isso pode ser feito atribuindo funções e permissões de usuário e usando a autenticação multifatorial ou outros métodos para verificar a identidade do usuário.
- Avaliações regulares de segurança: podem ajudar as organizações a identificar e resolver problemas de segurança e corrigi-los de forma proativa. Essas avaliações podem ser conduzidas por equipes de segurança internas ou por empresas de segurança externas.

As arquiteturas Zero Trust adotam uma abordagem abrangente para a proteção de dados, implementando várias medidas de segurança. Essas medidas incluem autenticação forte, criptografia de dados e controles de acesso granulares. Essa abordagem minimiza o risco de eventos de segurança relacionados a dados e protege informações confidenciais contra acesso não autorizado.

Resposta eficiente a incidentes

As organizações podem detectar e responder a eventos de segurança com mais rapidez e eficácia estabelecendo estruturas de monitoramento e resposta a incidentes no ambiente de nuvem. As arquiteturas Zero Trust enfatizam o monitoramento contínuo, a integração da inteligência de ameaças e a visibilidade em tempo real das atividades do usuário, do tráfego da rede e do comportamento do sistema. As equipes de segurança podem então identificar e mitigar os eventos de segurança de forma proativa. Essa abordagem reduz o tempo de detecção e resposta a possíveis problemas e minimiza o impacto nas operações de negócios. Os pontos principais incluem:

- Teste: independentemente da estrutura ou da metodologia de resposta a incidentes à qual sua organização se alinha, você deve testar seu plano de resposta a incidentes regularmente. Exercícios teóricos, simulações e equipes vermelhas oferecem oportunidades de praticar a resposta a incidentes em ambientes realistas, descobrir lacunas de ferramentas e capacidades e aumentar a experiência e a confiança dos respondentes a incidentes.
- Monitoramento: monitore continuamente seus ambientes de nuvem em busca de sinais de atividade anormal. Você pode fazer isso usando uma variedade de ferramentas e técnicas, como análise de log, monitoramento de rede e verificação de vulnerabilidade.
- Integração da inteligência de ameaças: integre a inteligência de ameaças às suas estruturas de monitoramento e resposta a incidentes. Isso ajudará sua organização a identificar e responder às ameaças com mais rapidez e eficácia.
- Visibilidade em tempo real: para identificar e responder rapidamente aos incidentes de segurança, sua organização precisa de visibilidade em tempo real das atividades do usuário, do tráfego da rede e do comportamento do sistema.
- Identificação e mitigação proativas: ao identificar e mitigar proativamente os eventos de segurança, sua organização pode reduzir o tempo de detecção e resposta a possíveis ameaças, minimizando o impacto nas operações de negócios.

Maior produtividade da força de trabalho

A força de trabalho moderna exige flexibilidade para realizar o trabalho em uma variedade cada vez maior de locais, dispositivos e horários. Ao implementar uma ZTA, você pode atender a esses requisitos e melhorar a mobilidade, a produtividade e a satisfação da força de trabalho, mantendo ou melhorando a postura de segurança da organização.

Ativar a transformação digital

As organizações estão buscando cada vez mais a interconexão de dispositivos, máquinas, instalações, infraestrutura e processos fora do perímetro da rede tradicional como parte da transformação digital. Os dispositivos de Internet das coisas (IoT) e tecnologia operacional (OT, também conhecida como Internet das Coisas Industrial, ou IIo T) geralmente transmitem informações de telemetria e manutenção preditiva diretamente para a nuvem. Para proteger as workloads, isso exige a aplicação de controles de segurança que vão além da abordagem tradicional de perímetro.

Resumo da seção

Ao se concentrar nesses resultados de negócios direcionados, sua organização pode aproveitar todo o potencial da ZTA e fortalecer a postura de segurança na nuvem. É importante alinhar esses resultados às metas organizacionais específicas, adaptá-los às suas necessidades comerciais exclusivas e avaliar regularmente a eficácia para impulsionar a melhoria contínua.

Noções básicas sobre os princípios Zero Trust

A arquitetura Zero Trust (ZTA) se baseia em um conjunto de princípios fundamentais que formam a base de seu modelo de segurança. Compreender esses princípios é essencial para organizações que buscam adotar uma estratégia ZTA de forma eficaz. Esta seção aborda os princípios fundamentais da ZTA.

Verificar e autenticar

O princípio de verificação e autenticação enfatiza a importância de uma identificação e autenticação fortes de entidades principais de todos os tipos, incluindo usuários, máquinas e dispositivos. A ZTA exige verificação contínua de identidades e status de autenticação durante toda a sessão, de preferência em cada solicitação. Ela não depende apenas do local ou dos controles tradicionais da rede. Isso inclui a implementação de uma autenticação multifator (MFA) moderna e forte, bem como a avaliação de sinais ambientais e contextuais adicionais durante os processos de autenticação. Ao adotar esse princípio, as organizações podem ajudar a garantir que as decisões de autorização de recursos tenham as melhores entradas de identidade possíveis.

Acesso de privilégio mínimo

O princípio do privilégio mínimo envolve conceder às entidades principais o nível mínimo de acesso necessário para realizar suas tarefas. Ao adotar o princípio do acesso com privilégio mínimo, as organizações podem aplicar controles de acesso granulares, para que as entidades principais tenham acesso somente aos recursos necessários para cumprir suas funções e responsabilidades. Isso inclui a implementação de provisionamento de just-in-time acesso, controles de acesso baseados em funções (RBAC) e análises regulares de acesso para minimizar a área de superfície e o risco de acesso não autorizado.

Microssegmentação

A microssegmentação é uma estratégia de segurança de rede que divide uma rede em segmentos menores e isolados para autorizar fluxos de tráfego específicos. Você pode obter a microssegmentação criando limites de workload e aplicando controles rígidos de acesso entre diferentes segmentos.

A microssegmentação pode ser implementada por meio de virtualização de rede, rede definida por software (SDN), firewalls baseados em host, listas de controle de acesso à rede () e AWS recursos específicosNACLs, como grupos de segurança do Amazon Elastic Compute Cloud (Amazon) ou. EC2 AWS PrivateLink Os gateways de segmentação controlam o tráfego entre os segmentos para autorizar explicitamente o acesso. Os gateways de microssegmentação e segmentação ajudam as organizações a restringir caminhos desnecessários na rede, especialmente aqueles que levam a sistemas e dados críticos.

Monitoramento e análise contínuos

O monitoramento e a análise contínuos envolvem a coleta, análise e correlação de eventos e dados relacionados à segurança em todo o ambiente da sua organização. Ao implementar ferramentas robustas de monitoramento e análise, sua organização pode avaliar dados de segurança e telemetria de forma convergente.

Esse princípio enfatiza a importância da visibilidade do comportamento do usuário, do tráfego da rede e das atividades do sistema para identificar anomalias e possíveis eventos de segurança. Tecnologias avançadas, como gerenciamento de informações e eventos de segurança (SIEM), análise de comportamento de usuários e entidades (UEBA) e plataformas de inteligência de ameaças, desempenham um papel vital na obtenção de monitoramento contínuo e detecção proativa de ameaças.

Automação e orquestração

A automação e a orquestração ajudam as organizações a simplificar os processos de segurança, reduzir a intervenção manual e melhorar os tempos de resposta. Ao automatizar tarefas rotineiras de segurança e usar recursos de orquestração, sua organização pode aplicar políticas de segurança consistentes e responder rapidamente a eventos de segurança. Esse princípio também inclui a automação dos processos de provisionamento e desprovisionamento de acesso para ajudar a garantir o gerenciamento oportuno e preciso das permissões do usuário. Ao adotar a automação e a orquestração, sua organização pode melhorar a eficiência operacional, reduzir os erros humanos e concentrar os recursos em iniciativas de segurança mais estratégicas.

Autorização

Em uma ZTA, cada solicitação para acessar um recurso deve ser explicitamente autorizada por um ponto de fiscalização. Além da identidade autenticada, as políticas de autorização devem considerar

contextos adicionais, como integridade e postura do dispositivo, padrões de comportamento, classificação de recursos e fatores de rede. O processo de autorização deve avaliar esse contexto convergente em relação às políticas de acesso correspondentes que são relevantes para o recurso que está sendo acessado. Preferencialmente, os modelos de machine learning podem fornecer um complemento dinâmico às políticas declarativas. Quando utilizados, esses modelos devem se concentrar apenas em restrições adicionais e não devem conceder acesso que não tenha sido especificado explicitamente.

Resumo da seção

Ao aderir a esses princípios fundamentais da ZTA, as organizações podem estabelecer um modelo de segurança robusto que se alinha à diversidade do ambiente corporativo moderno. A implementação desses princípios exige uma abordagem abrangente que combine tecnologia, processos e pessoas para alcançar uma mentalidade de confiança zero e criar uma postura de segurança resiliente.

Principais componentes de uma arquitetura de confiança zero

Para implementar uma estratégia de arquitetura de confiança zero (ZTA) de forma eficaz, sua organização deve entender os principais componentes que formam uma ZTA. Esses componentes trabalham juntos para melhorar continuamente um modelo de segurança abrangente que se alinha aos princípios Zero Trust. Esta seção aborda os principais componentes de uma ZTA.

Gerenciamento de identidade e acesso

O gerenciamento de identidade e acesso forma a base de uma ZTA, fornecendo autenticação de usuário e mecanismos gerais de controle de acesso robustos. Ele inclui tecnologias como autenticação única (SSO), autenticação multifator (MFA) e soluções de gerenciamento e governança de identidade. O gerenciamento de identidade e acesso fornece um alto nível de garantia de autenticação e um contexto importante que são essenciais para tomar decisões de autorização de confiança zero. Ao mesmo tempo, a ZTA é um modelo de segurança no qual o acesso a aplicações e recursos é concedido por usuário, por dispositivo e por sessão. Isso ajuda a proteger as organizações contra acesso não autorizado, mesmo que as credenciais do usuário estejam comprometidas.

Secure Access Service Edge

O Secure Access Service Edge (SASE) é uma nova abordagem à segurança de rede que virtualiza, combina e distribui funções de rede e segurança em um único serviço baseado em nuvem. O SASE pode fornecer acesso seguro a aplicações e recursos, independentemente da localização do usuário.

O SASE inclui uma variedade de recursos de segurança, como gateways web seguros, firewall como serviço e acesso à rede de confiança zero (ZTNA). Esses recursos funcionam juntos para proteger as organizações de uma ampla variedade de ameaças, incluindo malware, phishing e ransomware.

Prevenção de perda de dados

As tecnologias de prevenção de perda de dados (DLP) podem ajudar as organizações a proteger dados confidenciais contra divulgação não autorizada. As soluções DLP monitoram e controlam dados em movimento e em repouso. Isso ajuda as organizações a definir e aplicar políticas

que evitem eventos de segurança relacionados a dados, ajudando a garantir que informações confidenciais permaneçam protegidas em toda a rede.

Gerenciamento de eventos e informações de segurança

As soluções de gerenciamento de eventos e informações de segurança (SIEM) coletam, agregam e analisam logs de eventos de segurança de várias fontes na infraestrutura de uma organização. Você pode usar esses dados para detectar incidentes de segurança, facilitar a resposta a incidentes e fornecer informações sobre possíveis ameaças e vulnerabilidades.

Especificamente em ZTA, a capacidade de uma solução SIEM de correlacionar e entender a telemetria relacionada de diferentes sistemas de segurança é fundamental para melhorar a detecção e a resposta a padrões anormais.

Catálogo de propriedade de recursos corporativos

Para conceder acesso adequado aos recursos corporativos, uma organização deve ter um sistema confiável que catalogue esses recursos e, principalmente, quem os possui. Essa fonte de verdade precisa fornecer fluxos de trabalho que facilitem as solicitações de acesso, as decisões de aprovação associadas e os atestados regulares das mesmas. Com o tempo, essa fonte de verdade conterá as respostas para “quem pode acessar o quê?” dentro da organização. Você pode usar as respostas para autorização, auditoria e conformidade.

Gerenciamento de endpoints unificados

Além de autenticar fortemente o usuário, uma ZTA também deve considerar a integridade, a postura e o estado do dispositivo do usuário para avaliar se o acesso aos dados e recursos corporativos é seguro. Uma plataforma de gerenciamento de endpoints unificados (UEM) fornece os seguintes recursos:

- Provisionamento de dispositivos
- Gerenciamento contínuo de configurações e patches
- Linha de base de segurança
- Relatório de telemetria
- Limpeza e retirada de dispositivos

Pontos de fiscalização baseados em políticas

Em uma ZTA, o acesso a cada recurso deve ser explicitamente autorizado por um ponto de fiscalização baseado em políticas de bloqueio. Inicialmente, esses pontos de fiscalização podem ser baseados nos pontos de fiscalização existentes nos sistemas de rede e identidade existentes. Os pontos de fiscalização podem se tornar cada vez mais capazes considerando a maior variedade de contextos e sinais que a ZTA fornece. A longo prazo, sua organização deve implementar pontos de fiscalização específicos da ZTA que operem em contexto convergente, integrem consistentemente os provedores de sinal, mantenham um conjunto abrangente de políticas e sejam aprimorados com a inteligência obtida da telemetria combinada.

Resumo da seção

Compreender esses componentes principais é essencial para as organizações que planejam adotar uma ZTA. Ao implementar esses componentes e integrá-los em um modelo de segurança coeso, sua organização pode estabelecer uma postura de segurança forte com base nos princípios da Zero Trust. As seções a seguir exploram a prontidão organizacional, as abordagens de adoção em fases e as práticas recomendadas que ajudam você a implementar com sucesso a ZTA em sua organização.

Avaliação da prontidão organizacional para a adoção da Zero Trust

A adoção de uma nova estratégia de arquitetura é uma tarefa significativa que requer planejamento cuidadoso e consideração dos fatores organizacionais. Esta seção se concentra nas principais considerações de prontidão organizacional para a adoção da Zero Trust em toda a empresa. Ao abordar essas considerações, sua organização pode preparar o caminho para uma postura de segurança mais forte e bem-sucedida.

Alinhamento e comunicação da liderança

O alinhamento e a comunicação da liderança são essenciais para a implementação bem-sucedida da Zero Trust. A liderança deve compreender os benefícios da Zero Trust e os recursos necessários. Os líderes também devem estar dispostos a fazer mudanças na cultura e nos processos da organização. A comunicação com os funcionários é necessária para criar confiança e adesão. Os funcionários precisam entender por que a organização está implementando a Zero Trust, o que isso significa para eles e como podem ajudar. A comunicação deve ser aberta, transparente e contínua.

Apoio e adesão da liderança

Para que a implementação da arquitetura zero trust (ZTA) seja bem-sucedida, é fundamental alinhar os principais investidores e executivos às metas, aos benefícios e às medidas de sucesso da arquitetura. Compartilhe a importância dos princípios Zero Trust para aprimorar a segurança e permitir a agilidade dos negócios, abandonando a segurança tradicional baseada em perímetro e adotando uma abordagem mais granular e centrada no usuário. Ao mudar para essa abordagem, sua organização pode se adaptar às mudanças e ameaças mais rapidamente. O alinhamento executivo estabelece o tom da organização e ajuda a superar uma possível resistência à mudança.

Comunicação transparente

Mantenha uma comunicação aberta e transparente com os funcionários durante todo o processo de implementação da Zero Trust. Explique a lógica, os benefícios e os resultados esperados da adoção e resolva as preocupações imediatamente. Forneça atualizações regulares sobre o progresso da implementação. Isso aumentará a adesão, reduzirá a resistência e criará confiança.

Desenvolvimento e treinamento de habilidades

Depois que a liderança estiver alinhada e a comunicação aberta, é importante desenvolver as habilidades e o conhecimento dos funcionários que implementarão a Zero Trust. Isso inclui entender os princípios Zero Trust, como implementá-los em seu trabalho e como responder a eventos de segurança. Ofereça oportunidades de treinamento e desenvolvimento para ajudar os funcionários a adquirir essas habilidades.

Conhecimento e habilidades em nuvem

Avalie as habilidades e as lacunas de conhecimento da organização em tecnologias de nuvem e princípios Zero Trust. Forneça programas de treinamento e desenvolvimento para aprimorar as habilidades dos funcionários e equipá-los com a experiência necessária para trabalhar de forma eficaz em um ambiente Zero Trust e centrado na nuvem. Para acompanhar a evolução das tecnologias e das práticas de segurança, promova uma cultura de aprendizado contínuo.

Cultura e conscientização de segurança

Avalie a cultura de segurança da organização. Avalie o nível de conscientização sobre segurança entre os funcionários, a compreensão das práticas recomendadas de segurança e a adesão a políticas e procedimentos. Identifique quaisquer lacunas no conhecimento de segurança. Considere a realização de programas de treinamento de conscientização sobre segurança para educar os funcionários sobre a importância da Zero Trust e suas funções na manutenção de um ambiente seguro.

Estrutura organizacional e funções

Para implementar com êxito a Zero Trust, estabeleça uma estrutura organizacional e funções eficazes. Isso inclui criar um Cloud Center of Excellence (CCoE), revisar e modificar as operações de segurança e atribuir funções e responsabilidades para gerenciamento de vulnerabilidades, resposta a incidentes e monitoramento de segurança.

Centro de Excelência da Nuvem

Estabeleça um CCo E para fornecer orientação, melhores práticas e supervisão das operações na nuvem. A CCo E é uma equipe ou grupo de indivíduos responsáveis por criar e implementar as melhores práticas, diretrizes e políticas de governança relacionadas à nuvem. O CCo E deve incluir representantes de diferentes unidades de negócios e equipes de TI para ajudar a garantir a

colaboração e o alinhamento. O CCo E desempenha um papel crucial na adoção dos princípios Zero Trust em cargas de trabalho hospedadas na nuvem. O CCo E também facilita o compartilhamento de conhecimento em toda a organização.

Operações de segurança

Para atender às necessidades de um ambiente Zero Trust, revise e modifique a organização atual de operações de segurança. Para melhorar os recursos de monitoramento, resposta a incidentes e inteligência de ameaças, considere a implementação de centros de operações de segurança (SOCs) ou provedores de serviços de segurança gerenciados (MSSPs). Estabeleça funções e responsabilidades para gerenciamento de vulnerabilidades, resposta a incidentes e monitoramento de segurança. Um processo de resposta a incidentes que funcione bem é fundamental para garantir que eventos de segurança menores possam ser detectados e corrigidos rapidamente para interromper a sequência de eventos. Isso ajuda a evitar que um evento menor evolua para um mais impactante.

Infraestrutura e arquitetura de TI

Examine a arquitetura e a infraestrutura de TI da sua empresa para encontrar quaisquer restrições ou dependências que possam afetar a adoção de uma abordagem Zero Trust. Avalie se as aplicações e os sistemas atuais são compatíveis com os componentes arquitetônicos de confiança zero necessários. Analise se são necessárias melhorias ou ajustes na infraestrutura para apoiar a implantação bem-sucedida dos princípios Zero Trust. Para cada aplicação ou sistema, considere se a Zero Trust é melhor implementada no local ou por meio de um esforço maior de modernização.

Gerenciamento de riscos, governança e controle de alterações

Para implementar com êxito a Zero Trust, estabeleça processos eficazes de gerenciamento de riscos, governança e controle de alterações. Isso inclui alinhar o gerenciamento de riscos aos princípios Zero Trust, desenvolver um plano de resposta a incidentes, trabalhar com os departamentos jurídico e de conformidade e estabelecer um processo de controle de alterações.

Gerenciamento de riscos

Examine a estratégia de gerenciamento de riscos em vigor em sua empresa e determine até que ponto ela segue os princípios Zero Trust. Analise a eficiência dos atuais sistemas de resposta a incidentes, medidas de segurança e procedimentos de avaliação de risco. Determine quais áreas precisam ser aprimoradas para se adequar à estratégia Zero Trust. Comece a desenvolver um

sistema automatizado de resposta a incidentes ou uma estrutura de monitoramento e análise contínuos para agilizar a resolução.

Processos de controle de alterações

Para ajudar a garantir que todas as modificações relacionadas à nuvem atendam aos requisitos de segurança e conformidade, estabeleça métodos eficazes de controle de alterações. Estabeleça um procedimento sistemático de gerenciamento de alterações que inclua análise de configuração de segurança, avaliações de risco, aprovações e documentação. Revise e audite as atualizações com frequência para preservar a integridade da arquitetura Zero Trust.

Monitoramento e avaliação

Para implementar com êxito a Zero Trust, sua organização deve monitorar e avaliar continuamente a postura de segurança. Isso inclui estabelecer indicadores-chave de desempenho (KPIs), monitorar e avaliar e promover uma cultura de melhoria contínua. KPIs Ao seguir essas etapas, as organizações podem garantir que a implementação da Zero Trust seja bem-sucedida e que estejam sempre trabalhando para melhorar a segurança.

Indicadores chave de performance

Estabeleça indicadores-chave de desempenho pertinentes (KPIs) para avaliar o sucesso e a eficácia da implantação do Zero Trust. Eles KPIs podem medir a satisfação do usuário, o progresso do equipamento e da implantação, a redução de custos, a observância da conformidade e o número de ocorrências de segurança. Para acompanhar o desenvolvimento geral e encontrar oportunidades de melhoria, monitore e avalie-as regularmente KPIs.

Melhoria contínua

Estabelecer sistemas para obter opiniões e insights dos investidores ajudará a promover uma cultura de melhoria contínua. Incentive os membros da equipe a oferecer ideias e propostas para melhorar a segurança, a eficácia e a experiência do usuário do ambiente de nuvem. Use esses dados para simplificar procedimentos, melhorar as medidas de segurança e estimular a inovação.

Resumo da seção

Ao considerar essas questões organizacionais e culturais, sua organização poderá promover um ambiente favorável para a adoção na nuvem de um modelo de segurança Zero Trust. A próxima

seção explora as abordagens de adoção em fases, fornecendo orientação sobre como implementar gradualmente os princípios do Zero Trust de maneira prática e gerenciável.

Cultivando uma mentalidade de confiança zero

A implementação do Zero Trust vai além das implementações técnicas. Isso requer uma mudança cultural dentro da sua organização. Promover uma mentalidade de Zero Trust envolve enfatizar os seguintes aspectos principais.

Educação e treinamento Zero Trust

Eduque os funcionários sobre os valores e as vantagens da arquitetura de confiança zero (ZTA). Forneça explicações técnicas e não técnicas dos conceitos e abordagens da ZTA por meio de sessões de treinamento, workshops e outros recursos. Incentive os membros da equipe a estarem cientes de suas responsabilidades em estabelecer e manter um paradigma de segurança Zero Trust.

Colaboração e comunicação

Promova a colaboração e a transparência em todas as equipes e departamentos envolvidos na implementação do ZTA. Para garantir que todos tenham uma compreensão completa do plano, promova a comunicação interfuncional, o compartilhamento de conhecimento e a troca de informações. Crie uma cultura de responsabilidade compartilhada em que todos reconheçam a importância de suas contribuições para a segurança geral da empresa.

Aprendizado e melhoria contínuos

Priorize o aprendizado e a melhoria contínuos no contexto do Zero Trust. Incentive os funcionários a se manterem atualizados sobre as últimas tendências, tecnologias e melhores práticas de segurança. Cultive uma cultura de inovação e experimentação na qual os funcionários sejam incentivados a explorar novas soluções e abordagens para fortalecer a postura de segurança da organização.

Métricas e responsabilidade

Estabeleça métricas claras e mecanismos de responsabilidade para medir a eficácia da estratégia Zero Trust. Defina os principais indicadores de desempenho (KPIs) que se alinhem às metas de segurança da organização e acompanhe regularmente o progresso. Responsabilize indivíduos e equipes por suas contribuições para a implementação e manutenção dos princípios de Zero Trust.

Resumo da seção

Ao abordar esses aspectos e cultivar uma mentalidade de Zero Trust, as organizações podem criar uma base sólida para a adoção e implementação bem-sucedidas do Zero Trust. Essa mudança cultural é essencial para ajudar todos na organização a entender a importância do Zero Trust e contribuir ativamente para seu sucesso.

A próxima seção explora as abordagens de adoção em fases, fornecendo orientação sobre como implementar gradualmente os princípios do Zero Trust de maneira prática e gerenciável.

Abordagem em fases para Zero Trust

A adoção de uma arquitetura Zero Trust (ZTA) requer planejamento e implementação cuidadosos. Recomendamos uma abordagem de adoção em fases para facilitar a transição e minimizar as interrupções nas operações comerciais. Esta seção fornece orientação sobre as principais fases envolvidas na adoção de uma ZTA.

Fase 1: avaliação e planejamento

A primeira fase da implementação Zero Trust é a avaliação e o planejamento. Essa fase é fundamental para o êxito da implementação geral, uma vez que envolve identificar e resolver quaisquer lacunas na postura de segurança atual da sua organização. Ao avaliar seu estado atual e definir seus objetivos de segurança, você pode estabelecer as bases para uma implementação bem-sucedida da Zero Trust.

Ao mesmo tempo, uma avaliação perfeitamente completa e precisa pode nem sempre ser realista. Para evitar a paralisação da análise que impede você de avançar para outras fases, prepare-se para compartimentalizar ou aceitar algum nível de imperfeição.

1. Avaliar o estado atual: avalie a infraestrutura, as políticas e os controles de segurança existentes. Identifique possíveis vulnerabilidades, lacunas na segurança e áreas em que a implementação dos princípios Zero Trust pode oferecer melhorias.
2. Definir objetivos de segurança: com base nas descobertas da avaliação do estado atual, defina objetivos de segurança que se alinhem aos princípios Zero Trust. Esses objetivos de segurança também devem se alinhar à estratégia geral de segurança da sua organização e tratar as vulnerabilidades e lacunas identificadas.
3. Projetar a arquitetura: desenvolva uma ZTA que esteja à altura das metas de segurança da sua organização. Essa arquitetura deve incluir os componentes necessários, como soluções de gerenciamento de identidade e acesso, mecanismos de segmentação de rede e sistemas de monitoramento contínuo. A arquitetura também deve ser escalável, adaptável e capaz de acomodar o crescimento futuro e os avanços tecnológicos. O ideal é que essa arquitetura seja representada em um formato que seja facilmente consumido pelas equipes responsáveis por implementá-la, como um modelo do AWS CloudFormation , não apenas como um documento ou diagrama.
4. Envolver os investidores: envolva todos os investidores, incluindo unidades de negócios, equipes de TI e equipes de segurança, para obter insights e alinhar seus objetivos com o plano

de implementação da ZTA. Incentive a colaboração e a comunicação para estabelecer uma compreensão compartilhada dos benefícios e requisitos da abordagem Zero Trust.

Fase 2: condução e implementação

A segunda fase da implementação da Zero Trust é a condução e a implementação. Essa fase envolve testar a ZTA em um ambiente controlado de pequena escala e, em seguida, implantá-la iterativamente em toda a organização. É importante educar os funcionários sobre as novas medidas de segurança e as funções deles na manutenção de um ambiente Zero Trust.

1. Conduzir a implantação: teste a ZTA em um ambiente controlado e de pequena escala. Implemente os componentes e controles de segurança necessários que foram definidos na fase de design da arquitetura. Monitore de perto a implantação piloto, obtenha feedback e faça os ajustes necessários. Seja flexível logo no início do processo, quando a Zero Trust deixar de ser um exercício hipotético e passar a ser um exercício com o qual você está construindo uma experiência real.
2. Implantar de forma iterativa: com base nas lições aprendidas com a implantação piloto, inicie a implantação iterativa da Zero Trust em toda a organização. Crie impulso por meio de um efeito volante que não exija uma campanha extensa para atingir uma massa crítica de implantação. Reserve mandatos de liderança ou escalonamentos para o final mais longo da implantação, onde eles possam ser necessários.
3. Fornecer treinamento aos usuários e aumentar a conscientização: oriente os funcionários sobre as novas medidas de segurança e suas funções na manutenção de um ambiente Zero Trust. Enfatize a importância de práticas seguras, como senhas fortes, autenticação multifatorial e atualizações regulares de segurança.
4. Gerenciar alterações: crie um plano abrangente de gerenciamento de alterações para tratar as alterações organizacionais e culturais associadas à adoção da Zero Trust. Comunique os benefícios e a lógica por trás da adoção aos funcionários e resolva quaisquer preocupações ou resistências. Forneça suporte e orientação contínuos para facilitar uma transição perfeita.

Fase 3: monitoramento e melhoria contínua

A terceira e última fase da implementação da Zero Trust é o monitoramento e a melhoria contínua. Essa fase envolve o estabelecimento de um programa abrangente de monitoramento e análise, a

criação de um plano abrangente de resposta a incidentes e a solicitação regular de feedback dos investidores e usuários.

1. Monitorar continuamente: estabeleça um programa abrangente de monitoramento e análise para avaliar continuamente a postura de segurança e detectar possíveis anomalias. Use ferramentas e tecnologias de segurança avançadas para monitorar o comportamento do usuário, o tráfego da rede e as atividades do sistema.
2. Planejar resposta a incidentes e remediação: crie um plano abrangente de resposta a incidentes que se alinhe aos princípios Zero Trust. Estabeleça caminhos claros de escalonamento, defina funções e responsabilidades e implemente mecanismos automatizados de resposta a incidentes sempre que possível. Teste e atualize regularmente o plano de resposta a incidentes.
3. Obter feedback e avaliação: solicite regularmente feedback dos investidores e dos usuários para obter informações sobre a eficácia da arquitetura Zero Trust (ZTA). Faça avaliações periódicas para medir o impacto na postura de segurança, na eficiência operacional e na experiência do usuário. Use o feedback e os resultados da avaliação para identificar áreas de melhoria. Espere que isso mude com o tempo e considere como as equipes de desenvolvimento implementarão essas atualizações com o mínimo de esforço ou interrupções. ZTAs

Resumo da seção

Ao seguir essa abordagem de adoção em fases, as organizações podem fazer a transição efetiva para uma ZTA e, ao mesmo tempo, minimizar riscos e interrupções. A próxima seção discute as melhores práticas para alcançar o sucesso com a implementação do Zero Trust, abordando as principais considerações e recomendações para CxOs, VPs, e gerentes seniores.

Práticas recomendadas para obter êxito com a Zero Trust

A adoção bem-sucedida da arquitetura de confiança zero (ZTA) exige uma abordagem estratégica e a adesão às práticas recomendadas. Esta seção apresenta um conjunto de melhores práticas para orientar CxOs e os gerentes seniores a alcançar o sucesso com a adoção do Zero Trust. VPs Seguindo essas recomendações, sua organização pode estabelecer uma base de segurança sólida e obter os benefícios de uma abordagem Zero Trust:

- Definir objetivos e resultados comerciais claros: defina claramente os objetivos e os resultados comerciais desejados das operações na nuvem. Alinhe esses objetivos aos princípios Zero Trust para criar uma base sólida de segurança e, ao mesmo tempo, permitir o crescimento e a inovação dos negócios.
- Fazer uma avaliação abrangente: faça uma avaliação abrangente da infraestrutura de TI, das aplicações e dos ativos de dados atuais. Identifique dependências, débitos técnicos e possíveis problemas de compatibilidade. Essa avaliação informará o plano de adoção e ajudará a priorizar as workloads com base na criticidade, na complexidade e no impacto nos negócios.
- Desenvolva um plano de adoção — incorpore um plano de adoção detalhado que descreva a step-by-step abordagem para mover cargas de trabalho, aplicativos e dados para a nuvem. Defina fases de adoção, cronogramas e dependências. Envolva os principais investidores e aloque os recursos adequadamente.
- Começar a criar cedo: sua capacidade de representar autenticamente a aparência da Zero Trust em sua organização aumentará substancialmente depois que você começar a criá-la e implantá-la (em vez de analisá-la e falar sobre ela).
- Obter patrocínio executivo: garanta patrocínio executivo e suporte para a implementação da Zero Trust. Envolva outros executivos de nível C para defender a iniciativa e alocar os recursos necessários. O comprometimento da liderança é essencial para promover as mudanças culturais e organizacionais necessárias para uma implementação bem-sucedida.
- Implementar uma estrutura de governança: crie uma estrutura de governança que defina funções, responsabilidades e processos de tomada de decisão para a implementação da Zero Trust. Defina claramente a responsabilidade e a propriedade de controles de segurança, gerenciamento de riscos e conformidade. Revise e atualize regularmente a estrutura de governança para se adaptar aos requisitos de segurança em evolução.
- Apoiar a colaboração multifuncional: incentive a colaboração e a comunicação entre diferentes unidades de negócios, equipes de TI e equipes de segurança. Crie uma cultura de

responsabilidade compartilhada para promover o alinhamento e a coordenação em toda a implementação da Zero Trust. Incentive interações frequentes, compartilhamento de conhecimento e resolução conjunta de problemas.

- Proteger seus dados e aplicações: Zero Trust não se trata apenas de usuários finais acessando recursos e aplicações. Os princípios Zero Trust também devem ser implementados dentro e entre as workloads. Aplique os mesmos princípios técnicos, ou seja, identidade forte, microssegmentação e autorização, usando também todo o contexto disponível no datacenter.
- Forneça defesa em profundidade — implemente uma defense-in-depth estratégia usando várias camadas de controles de segurança. Combine várias tecnologias de segurança, como autenticação multifator (MFA), segmentação de rede, criptografia e detecção de anomalias, para fornecer proteção abrangente. Certifique-se de que cada camada complemente as outras para criar um sistema de defesa forte.
- Exigir autenticação forte: aplique mecanismos de autenticação forte, como MFA, para todos os usuários que acessam todos os recursos. Idealmente, considere a MFA moderna, como chaves de segurança FIDO2 suportadas por hardware, que fornece um alto nível de garantia de autenticação para Zero Trust e traz amplos benefícios de segurança (por exemplo, proteção contra phishing).
- Centralizar e melhorar a autorização: autorize especificamente cada tentativa de acesso. Dependendo das especificidades do protocolo, isso deve ser feito por conexão ou por solicitação. O ideal é por solicitação. Use todo o contexto disponível, incluindo informações de identidade, dispositivo, comportamento e rede, para tomar decisões de autorização mais granulares, adaptáveis e sofisticadas.
- Usar o princípio de privilégio mínimo: implemente o princípio de privilégio mínimo para conceder aos usuários os direitos de acesso mínimos necessários para realizar suas tarefas. Revise e atualize regularmente as permissões de acesso com base nas funções, responsabilidades e necessidades de negócios. Implemente just-in-time o provisionamento de acesso.
- Usar gerenciamento de acesso privilegiado: implemente uma solução de gerenciamento de acesso privilegiado (PAM) para proteger contas privilegiadas e reduzir o risco de acesso não autorizado a sistemas críticos. As soluções PAM podem fornecer controles de acesso privilegiado, gravação de sessão e recursos de auditoria para ajudar sua organização a proteger dados e sistemas mais confidenciais.
- Usar microssegmentação: divida sua rede em segmentos menores e mais isolados. Use a microssegmentação para impor controles rígidos de acesso entre segmentos com base nas funções do usuário, nas aplicações ou na confidencialidade dos dados. Esforce-se para eliminar todos os caminhos de rede desnecessários, especialmente aqueles que levam aos dados.

- Monitorar e responder aos alertas de segurança: implemente um programa abrangente de monitoramento de segurança e resposta a incidentes no ambiente de nuvem. Use ferramentas e serviços de segurança nativos de nuvem para detectar ameaças em tempo real, analisar logs e automatizar a resposta a incidentes. Estabeleça procedimentos claros de resposta a incidentes, conduza avaliações regulares de segurança e monitore continuamente anomalias ou atividades suspeitas.
- Usar monitoramento contínuo: para detectar e responder a incidentes de segurança de forma rápida e eficaz, implemente o monitoramento contínuo. Use ferramentas avançadas de análise de segurança para monitorar o comportamento do usuário, o tráfego da rede e as atividades do sistema. Automatize alertas e notificações para garantir que os incidentes sejam respondidos em tempo hábil.
- Promover uma cultura de segurança e conformidade: promova uma cultura de segurança e conformidade em toda a organização. Eduque os funcionários sobre práticas recomendadas de segurança, a importância de aderir aos princípios Zero Trust e o papel dos funcionários na manutenção de um ambiente de nuvem seguro. Realize treinamentos regulares de conscientização sobre segurança para ajudar a garantir que os funcionários estejam atentos à engenharia social e que entendam suas responsabilidades em relação à proteção e privacidade de dados.
- Usar simulações de engenharia social: faça simulações de engenharia social para avaliar a suscetibilidade do usuário a ataques de engenharia social. Use os resultados das simulações para personalizar os programas de treinamento a fim de melhorar a conscientização do usuário e a resposta a possíveis ameaças.
- Promover a educação contínua: estabeleça uma cultura de educação e aprendizado contínuos fornecendo treinamento e recursos de segurança permanentes. Mantenha os usuários informados sobre práticas recomendadas de segurança em evolução. Incentive os usuários a permanecerem vigilantes e denunciarem imediatamente quaisquer atividades suspeitas.
- Avaliar e otimizar continuamente: avalie regularmente o ambiente de nuvem em busca de áreas de melhoria. Use ferramentas nativas de nuvem para monitorar o uso e a performance dos recursos e realizar avaliações de vulnerabilidade e testes de penetração para identificar e resolver quaisquer pontos fracos.
- Estabelecer uma estrutura de governança e conformidade: desenvolva uma estrutura de governança e conformidade para ajudar a garantir que sua organização esteja alinhada aos padrões do setor e aos requisitos regulatórios. Na estrutura, defina políticas, procedimentos e controles para proteger dados e sistemas contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição. Implemente mecanismos para rastrear e gerar relatórios

sobre métricas de conformidade, realizar auditorias regulares e tratar prontamente quaisquer problemas de não conformidade.

- Incentivar a colaboração e o compartilhamento de conhecimento: incentive a colaboração e o compartilhamento de conhecimento entre as equipes envolvidas na adoção da ZTA. Você pode fazer isso promovendo a comunicação interfuncional e a colaboração entre TI, segurança e unidades de negócios. Sua organização também pode estabelecer fóruns, workshops e sessões de compartilhamento de conhecimento para promover a compreensão, enfrentar desafios e compartilhar lições aprendidas durante todo o processo de adoção.

Principais conclusões

Este guia explorou os aspectos essenciais do desenvolvimento de uma estratégia bem-sucedida de arquitetura de confiança zero (ZTA). Esta seção resume as principais conclusões da orientação prescritiva apresentada:

- Entender os princípios Zero Trust: é um modelo conceitual e um conjunto associado de mecanismos cujo foco é fornecer controles de segurança aos ativos digitais que não dependem única ou fundamentalmente dos tradicionais controles ou perímetros de rede. Em vez disso, os controles de rede são aumentados com identidade, dispositivo, comportamento e outros contextos e sinais ricos para tomar decisões de acesso mais granulares, inteligentes, adaptáveis e contínuas. Familiarize-se com os princípios fundamentais da Zero Trust, como privilégio mínimo, microssegmentação, autenticação contínua e autorização adaptativa.
- Definir objetivos claros: defina claramente os objetivos e os resultados comerciais desejados da adoção da ZTA. Alinhe esses objetivos aos princípios Zero Trust para ajudar a garantir uma base sólida de segurança e, ao mesmo tempo, permitir o crescimento e a inovação dos negócios.
- Fazer avaliações abrangentes: faça uma avaliação completa da sua infraestrutura de TI, das aplicações e dos ativos de dados existentes. Identifique dependências, débitos técnicos e problemas de compatibilidade para embasar sua estratégia de adoção.
- Desenvolva um plano de adoção do ZTA — Crie um plano detalhado que descreva a step-by-step abordagem para mover cargas de trabalho, aplicativos e dados para a nuvem. Considere fatores como requisitos de conformidade e modernização de aplicações.
- Implementar uma ZTA robusta: projete e implemente uma ZTA que aplique controles de acesso granulares, mecanismos de autenticação forte e monitoramento contínuo. Para uma adoção mais eficiente do ZTA, use serviços Zero Trust nativos da nuvem, como o Acesso Verificado pela AWS Amazon VPC Lattice.
- Priorizar a segurança de dados e aplicações: aplique os princípios Zero Trust, que são identidade forte, microssegmentação e autorização, para fornecer todo o contexto disponível. Use esse contexto para usuários que acessam sistemas e recursos e para o fluxo de comunicações e dados dentro e entre os componentes de back-end.
- Estabelecer estruturas de monitoramento e resposta a incidentes: implemente recursos robustos de monitoramento de segurança e resposta a incidentes no ambiente de nuvem. Use ferramentas de segurança nativas da nuvem para detecção de ameaças em tempo real, análise de registros e automação de resposta a incidentes, como Amazon Inspector AWS Security Hub e Amazon. GuardDuty

- Promover uma cultura de segurança e conformidade: promova uma cultura de conscientização e conformidade sobre segurança em toda a organização. Eduque os funcionários sobre práticas recomendadas de segurança e seu papel na manutenção de um ambiente de nuvem seguro.
- Avaliar e otimizar continuamente: avalie regularmente o ambiente de nuvem, os controles de segurança e os processos operacionais. Para coletar insights e otimizar a utilização de recursos, o gerenciamento de custos e o desempenho, use ferramentas de análise e monitoramento nativas da nuvem, como Amazon e. CloudWatch AWS Security Hub
- Estabelecer estruturas de governança e conformidade: desenvolva estruturas de governança e conformidade que se alinhem aos padrões do setor e aos requisitos regulatórios. Defina políticas, procedimentos e controles para ajudar a garantir a adesão aos padrões de segurança, privacidade e conformidade.

Próximas etapas

A adoção de uma arquitetura zero trust (ZTA) é uma das formas mais seguras de melhorar a postura da sua organização e reduzir os riscos. Esta orientação prescritiva contém um roteiro abrangente para a implementação da Zero Trust, desde a compreensão dos princípios até a avaliação de sua prontidão e a implementação dos componentes necessários.

As próximas etapas nesse fluxo de trabalho ou domínio envolvem o seguinte:

- Implementação do plano de adoção
- Implementação da ZTA
- Realização de avaliações regulares de segurança
- Otimização contínua do ambiente de nuvem e dos controles de segurança

ZTA é um processo contínuo que exige monitoramento, avaliação e adaptação constantes para garantir uma base de segurança sólida. Ao seguir as práticas recomendadas descritas nesta orientação, sua organização pode aprimorar a postura de segurança, garantir a conformidade com os regulamentos e proteger dados confidenciais.

Perguntas frequentes

Esta seção fornece respostas para perguntas comuns sobre a criação e a implementação de uma arquitetura de confiança zero (ZTA).

O que é Zero Trust?

Zero trust é um modelo conceitual e um conjunto associado de mecanismos cujo foco é fornecer controles de segurança aos ativos digitais que não dependem única ou fundamentalmente dos tradicionais controles ou perímetros de rede. Em vez disso, os controles de rede são aumentados com identidade, dispositivo, comportamento e outros contextos e sinais ricos para tomar decisões de acesso mais granulares, inteligentes, adaptáveis e contínuas.

O que Serviços da AWS pode me ajudar a implementar a arquitetura de confiança zero?

AWS fornece vários serviços que podem auxiliar na implementação do Zero Trust, como AWS Identity and Access Management (IAM) Acesso Verificado pela AWS, Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway e Amazon. GuardDuty

Como posso garantir a segurança de dados com a AWS?

AWS oferece serviços como AWS Key Management Service (AWS KMS) para criptografia de dados em repouso e em trânsito, Amazon Virtual Private Cloud (Amazon VPC) para isolamento de rede e AWS Secrets Manager para armazenamento e recuperação seguros de credenciais.

Pode AWS ajudar com os requisitos de conformidade em um ambiente Zero Trust?

Sim, AWS tem programas e serviços de conformidade para ajudar a atender a vários requisitos regulatórios. AWS Artifact fornece acesso a relatórios de AWS conformidade e AWS Config oferece suporte ao monitoramento e avaliação contínuos da conformidade.

Existem AWS ferramentas ou serviços para automatizar a segurança em um ambiente Zero Trust?

AWS fornece serviços como AWS Security Hub, por exemplo, que centraliza e automatiza as descobertas de segurança e AWS Config regras para definir e aplicar políticas de segurança.

Como posso garantir o monitoramento contínuo e a resposta a incidentes em um ambiente de nuvem Zero Trust com AWS

AWS oferece serviços como o Amazon CloudWatch para monitoramento em tempo real e AWS CloudTrail para registro e análise. Para obter as práticas recomendadas de resposta a incidentes, você pode usar o AWS Security Incident Response Guide.

Recursos

Referências

- What is a cloud center of excellence and why should your organization create one? — Esta postagem do blog fornece uma visão geral do CCo E, das melhores práticas para criar um CCo E eficaz e muito mais.
- Zero Trust on AWS — Esta página fornece uma visão geral dos princípios de segurança Zero Trust e das melhores práticas no AWS ambiente.
- Arquitetura Zero Trust: Uma AWS perspectiva — Esta postagem do blog compartilha uma definição e princípios orientadores da forma como o Zero Trust é implementado em AWS.
- AWS Identity and Access Management Guia do usuário (IAM) — Este guia oferece documentação abrangente sobre como gerenciar o acesso e as permissões do usuário no IAM, um componente crucial da arquitetura de confiança zero.
- AWS Security Hub— Saiba mais sobre o Security Hub, um serviço que fornece uma visão abrangente dos alertas de segurança e do status de conformidade em todo o seu Contas da AWS.
- AWS Well-Architected Framework: explore o Well-Architected Framework, que oferece orientação sobre como criar arquiteturas seguras, de alta performance, resilientes e eficientes na AWS.
- AWS Guia de resposta a incidentes de segurança — Este guia apresenta uma visão geral dos fundamentos da resposta a incidentes de segurança no ambiente da sua organização. Nuvem AWS Ele fornece uma visão geral dos conceitos de segurança e resposta a incidentes na nuvem e identifica recursos, serviços e mecanismos de nuvem que estão disponíveis para clientes que respondem a problemas de segurança.

Ferramentas

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- Acesso Verificado pela 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
Atualizações adicionadas	Foram adicionadas informaçõ es à seção Principais componentes de uma arquitetura de confiança zero, foram feitas alterações na seção Avaliação da prontidão organizacional para a adoção da Zero Trust, foram adicionad as informações à seção Práticas recomendadas e foram feitas alterações nas Perguntas frequentes.	4 de dezembro de 2023
Publicação inicial	—	19 de junho de 2023

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migre seu banco de dados Oracle local para a edição compatível com o Amazon Aurora PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para o. AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

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

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

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações 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.