Criar uma estratégia de criptografia corporativa para dados em repouso

AWS Orientação prescritiva

AWS Orientação prescritiva: Criar uma estratégia de criptografia corporativa para dados em repouso

Table of Contents

Criar uma estratégia de criptografia corporativa para dados em repouso

Venki Srivatsav, Andrea Di Fabio e Vikramaditya Bhatnagar, da Amazon Web Services ()AWS

Setembro de 2022 (histórico do documento)

Muitas empresas estão preocupadas com a ameaça à segurança cibernética de uma violação de dados. Quando ocorre uma violação de dados, uma pessoa não autorizada obtém acesso à sua rede e rouba dados corporativos. Firewalls e serviços antimalware podem ajudar a proteger contra essa ameaça. Outra proteção que você pode implementar é a criptografia de dados. Na seção Sobre a criptografia de dados deste guia, você pode aprender mais sobre como a criptografia de dados funciona e os tipos disponíveis.

Quando você está discutindo criptografia, de um modo geral, existem dois tipos de dados. Dados em trânsito que estão se movendo ativamente pela sua rede, como entre os recursos da rede. Dados em repouso são dados estacionários e inativos, como dados armazenados. Essa estratégia se concentra nos dados em repouso. Para obter mais informações sobre a criptografia de dados em trânsito, consulte Proteção de dados em trânsito (AWS Well-Architected Framework).

Uma estratégia de criptografia consiste em quatro partes que você desenvolve em fases sequenciais. A política de criptografia é determinada pela gerência sênior e descreve os requisitos normativos, de conformidade e de negócios para criptografia. Os padrões de criptografia ajudam aqueles que implementam a política a entendê-la e cumpri-la. Os padrões podem ser tecnológicos ou processuais. A estrutura são os procedimentos operacionais, estruturas e grades de proteção padrão que apoiam a implementação dos padrões. Por fim, a arquitetura é a implementação técnica de seus padrões de criptografia, como o ambiente, os serviços e as ferramentas que você usa. O objetivo deste documento é ajudá-lo a criar uma estratégia de criptografia adequada às suas necessidades comerciais, de segurança e de conformidade. Ele inclui recomendações sobre como revisar e implementar padrões de segurança para dados em repouso, para que você possa atender às suas necessidades comerciais e de conformidade de forma holística.

Essa estratégia usa AWS Key Management Service (AWS KMS) para ajudá-lo a criar e gerenciar chaves criptográficas que ajudam a proteger seus dados. AWS KMS se integra a vários AWS serviços para criptografar todos os seus dados em repouso. Mesmo se você escolher um serviço de criptografia diferente, ainda poderá adotar as recomendações e as fases deste guia.

Público-alvo

A estratégia foi projetada para atender aos seguintes públicos:

- Diretores executivos que formulam políticas para sua empresa CEOs, como diretores de tecnologia (CTOs), diretores de informações (CIOs) e diretores de segurança da informação (CISOs)
- Líderes de tecnologia responsáveis pela definição de padrões técnicos, como vice-presidentes e diretores técnicos
- Diretores de conformidade e governança encarregados de monitorar a adesão às políticas de conformidade, incluindo regimes de conformidade estatutários e voluntários

Resultados de negócios desejados

- Data-at-rest política de criptografia — os tomadores de decisão e os formuladores de políticas podem criar uma política de criptografia e entender os fatores críticos que afetam a política.
- Data-at-rest padrões de criptografia — Os líderes técnicos podem desenvolver padrões de criptografia baseados na política de criptografia.
- Estrutura para criptografia — Líderes técnicos e implementadores podem criar uma estrutura que atue como uma ponte entre aqueles que determinam a política e aqueles que criam os padrões. Estrutura, nesse contexto, significa identificar o processo e o fluxo de trabalho apropriados que ajudam a implementar os padrões dentro dos limites da política. Uma estrutura é semelhante a um procedimento operacional padrão ou a um processo de gerenciamento de mudanças para alterar políticas ou padrões.
- Arquitetura técnica e implementação — implementadores práticos, como desenvolvedores e arquitetos, estão cientes das referências de arquitetura disponíveis que podem ajudá-los a implementar a estratégia de criptografia.

Limitações

O objetivo deste documento é ajudá-lo a formular uma estratégia de criptografia personalizada que melhor atenda às necessidades da sua empresa. Não é uma estratégia de criptografia em si e não é uma lista de verificação de conformidade. Os tópicos a seguir não estão incluídos neste documento:

- Criptografia de dados em trânsito

- Tokenização
- Hashing
- Conformidade e governança de dados
- Orçamento para seu programa de criptografia

Para obter mais informações sobre alguns desses tópicos, consulte a Recursos seção.

Sobre a criptografia de dados

Esta seção contém uma visão geral de alto nível dos conceitos e terminologia de criptografia. A criptografia de dados ajuda você a impor a confidencialidade dos dados. Ao implementar controles de criptografia e acesso, você pode ajudar a proteger os dados em sua empresa.

Sobre as chaves de criptografia

Os serviços de criptografia usam uma chave de criptografia para criptografar dados. Uma chave de criptografia é uma sequência criptográfica de bits aleatórios gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva. A força da criptografia geralmente depende de dois fatores: o comprimento da chave e o algoritmo usado. Em geral, chaves mais longas fornecem criptografia mais forte.

Sobre algoritmos de criptografia

Existem dois tipos de algoritmos para gerar chaves de criptografia, simétricos e assimétricos.

A criptografia simétrica usa a mesma chave para criptografar e descriptografar os dados. Esse tipo de criptografia geralmente é mais rápido e, portanto, eficiente para grandes quantidades de dados. Esse tipo de criptografia é amplamente usado e geralmente aceito como seguro. Como uma única chave é usada tanto para criptografia quanto para decodificação, a melhor prática é alterar a chave com frequência para evitar que uma pessoa não autorizada a obtenha. Para obter mais informações sobre quando a criptografia simétrica é recomendada, consulte a Quando eu preciso de criptografia simétrica? seção Perguntas frequentes.

A criptografia simétrica 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. A criptografia assimétrica geralmente é considerada mais segura do que a criptografia simétrica, mas é mais lenta porque usa comprimentos de chave maiores e requer cálculos de criptografia mais complexos. Para obter mais informações sobre quando a criptografia assimétrica é recomendada, consulte a Quando eu preciso de criptografia assimétrica? seção Perguntas frequentes.

Sobre a criptografia de envelope

Quando você criptografa seus dados, eles são protegidos somente enquanto sua chave de criptografia permanece secreta. A chave usada para criptografar os dados é conhecida como chave de dados. A criptografia de envelope é a prática de criptografar sua chave de dados com outra chave de criptografia, chamada chave de criptografia de chave. Você pode até mesmo criptografar essa chave com outra chave de criptografia e assim por diante. Eventualmente, uma chave deve permanecer em texto simples para que você possa descriptografar as chaves e seus dados. Essa chave de criptografia em texto simples de nível superior é chamada de chave raiz.

A criptografia de envelope oferece vários benefícios:

- Conveniência — Como sua chave de dados é criptografada, você pode armazená-la com os dados criptografados.
- Eficiência — As operações de criptografia podem ser demoradas, principalmente quando se trata de uma grande quantidade de dados. Em vez de recriptografar dados brutos várias vezes com diferentes chaves, você pode recriptografar somente as chaves de dados que protegem os dados brutos. Isso permite que você forneça duas ou mais camadas de proteção de criptografia sem recriptografar os dados.
- Desempenho — Você pode combinar algoritmos de criptografia. Por exemplo, você pode usar criptografia simétrica para os dados brutos, mas usar criptografia assimétrica para a chave de dados, que combina os pontos fortes dos dois algoritmos de criptografia.

Para obter mais informações sobre criptografia de envelope, consulte Criptografia de envelope (AWS Key Management Service documentação). Para obter mais informações sobre como decidir se você precisa de criptografia de envelope, consulte a Quando eu preciso de criptografia de envelope? seção Perguntas frequentes.

Fases da criação de uma estratégia de criptografia

A criação de uma estratégia de criptografia em nível corporativo requer uma abordagem em várias fases. Cada fase define um conjunto de controles para ajudá-lo a alcançar os resultados desejados e tangíveis. Este documento orienta você nessas fases e faz perguntas específicas para ajudá-lo a personalizar sua estratégia de criptografia.

A criação de uma estratégia de criptografia para dados em repouso consiste nas seguintes fases sequenciais:

1. Política de criptografia— crie uma política que defina os objetivos de data-at-rest criptografia para sua empresa.
2. Padrões de criptografia— defina os padrões técnicos e processuais que ajudam você a concretizar sua política empresarial.
3. Estrutura de criptografia— crie a estrutura que ajude todas as partes interessadas a entender, alterar e implementar seus padrões de criptografia.
4. Implementação— Implante sua infraestrutura de criptografia.

Política de criptografia

O objetivo de uma política de criptografia é estabelecer, em nível de gerência sênior, as expectativas comerciais e de conformidade que a organização precisa atender. A política serve como ponto de partida para definir uma estratégia de criptografia adequada. A política deve ser abstrata o suficiente para fornecer liberdade e flexibilidade para implementação. Ao mesmo tempo, deve ser específico o suficiente para definir os limites de uma implementação aceitável que atenda aos objetivos organizacionais. Em geral, as políticas são independentes da tecnologia e são alteradas com pouca frequência porque definem as características fundamentais da estratégia de criptografia da sua empresa.

Normalmente, as políticas de criptografia contêm, mas não estão limitadas ao seguinte:

- Qualquer regime regulatório ou de conformidade que sua empresa deva cumprir
- Quaisquer compromissos ou expectativas comerciais em relação à criptografia de dados
- O tipo de dados que devem ser criptografados

- Critérios para quando usar técnicas de proteção de dados que não sejam criptografia, como hashing ou tokenização

O nível mais alto de gerenciamento da organização, como CIO, CTO e CISO, geralmente define e aprova a política de criptografia.

Considere o seguinte ao criar sua política de criptografia:

- Sua linha de negócios determina os regimes regulatórios e de conformidade que você precisa seguir. Esses regimes ditam os requisitos de criptografia de dados. Decisões de nível executivo para expandir os negócios para novas regiões ou expandir as ofertas de produtos podem afetar quais regulamentações se aplicam aos seus dados. Por exemplo, se um banco decidir oferecer cartões de crédito a seus clientes, provavelmente precisará estar em conformidade com o Padrão de Segurança de Dados do setor de cartões de pagamento (PCI-DSS), que exige criptografia de dados.
- Sua política deve especificar quais tipos de dados precisam ser criptografados. Isso varia de acordo com os requisitos de conformidade e os objetivos de tratamento de dados de sua empresa. Por exemplo, sua política pode indicar que todos os dados que a empresa captura ou possui devem ser criptografados em repouso.
- Sua política de criptografia deve estar alinhada com seus padrões internos de categorização de dados. Para formular uma política de criptografia eficaz, é necessária a determinação das categorias de dados no nível dos metadados. Por exemplo, suas categorias podem incluir dados públicos, internos, confidenciais, secretos ou de clientes.
- Inclua critérios para determinar quais dados devem ser criptografados e quais dados devem ser protegidos com outra técnica, como tokenização ou hashing. Por exemplo, sua política pode indicar que qualquer informação de identificação pessoal (PII) que vá para os registros de auditoria, rastreamento ou aplicativo deve ser tokenizada.

Padrões de criptografia

Os padrões são derivados de sua política. Eles têm um escopo mais restrito e ajudam a definir a estrutura e a arquitetura para implementação. Por exemplo, se a política da sua organização é criptografar seus dados em repouso, um padrão definiria o tipo de criptografia necessária e forneceria orientações gerais sobre como aderir à política.

Os padrões de criptografia geralmente especificam o seguinte:

- Os tipos de criptografia que devem ser usados
- Especificações mínimas para chaves de criptografia
- Quem tem acesso às chaves de criptografia
- Onde as chaves de criptografia devem ser armazenadas
- Critérios para escolher uma força de chave apropriada ao escolher técnicas de criptografia ou hashing
- Frequência de rotação da chave

Embora você raramente precise atualizar uma política de criptografia, os padrões de criptografia estão sujeitos a alterações. O setor de cibersegurança evolui constantemente para atender ao cenário de ameaças em constante mudança. Dessa forma, seus padrões devem mudar para adotar as tecnologias e práticas recomendadas mais recentes, a fim de fornecer a melhor proteção possível para seus dados corporativos.

Em uma organização corporativa, vice-presidentes, diretores ou administradores de dados geralmente definem padrões de criptografia, e um oficial de conformidade normalmente os revisa e aprova.

Considere as seguintes categorias de fatores ao definir e manter os padrões de criptografia em sua organização:

- Considerações de custo e desempenho
- Controle de acesso por chave
- Tipos de criptografia
- Especificações da chave de criptografia
- Local de armazenamento da chave

Considerações de custo e desempenho

Considere os seguintes fatores operacionais ao determinar os padrões de criptografia para dados em repouso:

- Os recursos de hardware disponíveis devem ser capazes de suportar seus padrões em grande escala.

- O custo da criptografia varia de acordo com o tamanho da chave, a quantidade de dados e o tempo necessário para realizar a criptografia. Por exemplo, quando comparada à criptografia simétrica, a criptografia assimétrica usa chaves mais longas e leva mais tempo.
- Considere os requisitos de desempenho de seus aplicativos corporativos. Se seu aplicativo exigir baixa latência e alta taxa de transferência, talvez você queira usar criptografia simétrica.

Controle de acesso por chave

Identifique políticas de controle de acesso para suas chaves de criptografia com base no princípio de privilégio mínimo. Privilégio mínimo é a prática recomendada de segurança para conceder aos usuários o acesso mínimo de que eles precisam para realizar suas funções de trabalho. Em seus padrões, defina uma política de controle de acesso que:

- Identifica as funções que gerenciam as chaves de criptografia de chaves e as chaves de dados.
- Define e mapeia as principais permissões para as funções. Por exemplo, ele define quem tem os principais privilégios de administrador e quem tem os principais privilégios de usuário. Os administradores de chaves podem criar ou modificar chaves de criptografia de chaves, e os usuários de chaves podem criptografar e descriptografar dados e gerar chaves de dados.

Tipos de criptografia

Em seus padrões, defina quais tipos e recursos de criptografia são adequados para sua organização:

- Documente quando usar algoritmos de criptografia simétrica e assimétrica. Para obter mais informações, consulte Quando eu preciso de criptografia simétrica? e Quando eu preciso de criptografia assimétrica? na seção de perguntas frequentes.
- Decida se você deve usar criptografia de envelope e defina as circunstâncias. Para obter mais informações, consulte a Quando eu preciso de criptografia de envelope? seção de perguntas frequentes.
- Defina critérios para quando usar alternativas de criptografia, como tokenização e hashing.

Especificações da chave de criptografia

Defina as especificações necessárias para suas chaves de criptografia, como a força da chave e os algoritmos. Essas especificações devem estar em conformidade com os regimes regulatórios e de conformidade definidos na política. Considere definir as seguintes especificações:

- Defina a força mínima da chave e os algoritmos para os tipos de criptografia simétrica e assimétrica. Os fatores de força chave incluem comprimento, aleatoriedade e exclusividade.
- Defina quando você deseja implementar novas versões dos algoritmos de criptografia. Por exemplo, seus padrões podem indicar Implementar a versão mais recente do algoritmo dentro de 30 dias após o lançamento ou Sempre usar uma versão anterior à versão mais recente.
- Defina o intervalo para rotação de suas chaves de criptografia.

Local de armazenamento da chave

Em seus padrões, considere o seguinte ao decidir onde armazenar suas chaves de criptografia:

- Os requisitos regulatórios e de conformidade podem determinar onde suas chaves de criptografia podem ser armazenadas.
- Decida se você deseja armazenar as chaves em um local centralizado ou com os dados correspondentes. Para obter mais informações, consulte a Por que eu deveria gerenciar centralmente as chaves de criptografia? seção de perguntas frequentes.
- Se você escolher o armazenamento centralizado, decida se deseja armazenar as chaves em uma infraestrutura gerenciada pela empresa, como um módulo de segurança de hardware (HSM), ou em um provedor de serviços gerenciados, como. AWS Key Management Service Para obter mais informações, consulte a Quando preciso usar um módulo de segurança de hardware (HSM)? seção de perguntas frequentes.

Estrutura de criptografia

Uma estrutura, nesse contexto, se refere a um conjunto de procedimentos operacionais padrão que precisam ser seguidos quando você modifica os padrões ou a política de criptografia. A estrutura é o andaime que ajuda você a implementar os padrões. Isso ajuda a converter palavras em ações. A estrutura vincula as pessoas que definem os padrões às pessoas que os implementam.

As estruturas geralmente incluem os seguintes tópicos:

Classificação de dados

A classificação de dados desempenha um papel vital na criação de uma estratégia de criptografia. A classificação de dados é o processo de atribuição de dados a uma categoria com base na sensibilidade dos dados. A seguir estão categorias comuns de classificação de dados, em ordem crescente de sensibilidade: pública, privada, interna, confidencial e restrita.

Sua estrutura de criptografia deve incluir as seguintes informações sobre classificação de dados:

- As categorias de classificação de dados para sua empresa.
- Os critérios de classificação usados para classificar os dados em sua categoria apropriada. Por exemplo, a receita comercial de uma empresa pode ser classificada como restrita, as PII dos funcionários podem ser confidenciais e a comunicação interna entre funcionários por meio de canais oficiais pode ser interna.
- O processo usado para promover e rebaixar dados entre categorias.
- Os critérios de acesso para cada categoria de classificação de dados.
- O tipo de chave de criptografia necessária para cada categoria.

Classificação do ambiente

Sua empresa pode ter vários ambientes, como desenvolvimento, teste, sandbox, pré-produção e produção. Cada ambiente pode conter tipos diferentes de dados e ter requisitos de criptografia diferentes.

Sua estrutura de criptografia deve incluir as seguintes informações sobre seus ambientes:

- Defina seus ambientes corporativos.
- Defina os requisitos de criptografia para cada ambiente. Por exemplo, você pode usar uma única chave de criptografia para todas as categorias de dados em seu ambiente de desenvolvimento e, em seu ambiente de produção, você pode usar chaves de criptografia diferentes para cada aplicativo comercial ou categoria de classificação de dados.

Eventos e processos de mudança

Os padrões de criptografia estão sujeitos a mudanças frequentes para que você possa acompanhar as tecnologias, as melhores práticas e as inovações mais recentes. A seguir estão os eventos de alteração comuns que podem iniciar uma revisão de seus padrões de criptografia:

- Alterações no tamanho mínimo das chaves de criptografia
- Mudanças na força de um algoritmo de criptografia
- Alterações em quem pode acessar as chaves de criptografia e como
- Alterações nos intervalos de rotação de suas teclas
- Alterações no processo de exclusão de chaves
- Alterações no local ou nas políticas de armazenamento de chaves
- Alterações no processo de backup e restauração de chaves

Sua estrutura de criptografia deve incluir o seguinte para ajudar a preparar sua organização para gerenciar, implementar e comunicar alterações nos padrões ou políticas de criptografia:

- Processo de controle de mudanças — O objetivo desse processo é planejar e se preparar para a próxima mudança. Quando você precisa alterar seus padrões ou políticas de criptografia, esse processo repetível e escalável foi projetado para definir:
  - Como sua organização avalia o impacto da mudança
  - Quem pode iniciar mudanças
  - Quem é responsável pela implementação da mudança
  - Quem é responsável por aprovar a mudança
  - Como sua organização reverteria a mudança, se necessário
- Processo de auditabilidade e rastreabilidade de alterações — Esse processo define como sua organização audita e rastreia as mudanças, tanto no nível dos metadados quanto no nível dos dados. Ele deve definir como você mantém e acessa registros de:
  - O que mudou
  - Quando foi alterado
  - Quem iniciou, aprovou e implementou a mudança

Por exemplo, se sua organização alterar a força mínima da chave de criptografia, você deverá ser capaz de determinar os requisitos originais e novos, quando a alteração entrou em vigor e quem esteve envolvido no processo de alteração.

- Processo de implantação de mudanças — O objetivo desse processo é definir como sua organização implementa a mudança depois de você decidir fazê-la. Esse processo define:
  - Quem são as partes interessadas
  - Se você deve concluir um piloto ou uma prova de conceito
  - Como e quando você deve comunicar o status da mudança
  - Como reverter a alteração, se necessário.
  - Qual deve ser o período de observação após a implementação da mudança.
  - Qual será o processo de observação para monitorar o impacto da mudança, incluindo como coletar feedback sobre a mudança e avaliar a eficácia
- Processo de aposentadoria — O objetivo desse processo é definir como sua organização lida com a retirada de recursos e informações relacionados à criptografia. Inclui instruções para a aposentadoria real, bem como o processo de comunicação para a aposentadoria.

Implementação

Nessa estratégia, a arquitetura se refere à implementação técnica de seus padrões de criptografia. Esta seção inclui informações sobre como Serviços da AWS, por exemplo, AWS Key Management Service (AWS KMS) e AWS CloudHSM, podem ajudá-lo a implementar sua estratégia de data-at-rest criptografia de acordo com sua política e padrões.

AWS KMS é um serviço gerenciado que ajuda você a criar e controlar as chaves criptográficas usadas para proteger seus dados. As chaves KMS nunca saem do serviço sem criptografia. Para usar ou gerenciar suas chaves KMS, você interage com AWS KMS, e muitas delas Serviços da AWS são integradas. AWS KMS

AWS CloudHSM é um serviço criptográfico para criar e manter módulos de segurança de hardware (HSMs) em seu AWS ambiente. HSMs são dispositivos de computação que processam operações criptográficas e fornecem armazenamento seguro para chaves criptográficas. Se seus padrões exigirem que você use hardware validado pelo FIPS 140-2 Nível 3, ou se seus padrões determinarem o uso de padrões do setor, como PKCS #11 APIs, Java Cryptography Extensions (JCE) e Microsoft CryptoNG (CNG), você pode considerar o uso. AWS CloudHSM

Você pode configurar AWS CloudHSM como um armazenamento de chaves personalizado para AWS KMS. Essa solução combina a conveniência e a integração de serviços AWS KMS com os benefícios adicionais de controle e conformidade do uso de um AWS CloudHSM cluster em seu Conta da AWS. Para obter mais informações, consulte Armazenamentos de chaves personalizadas (AWS KMS documentação).

Este documento discute os AWS KMS recursos em alto nível e explica como AWS KMS abordar sua política e seus padrões.

Custo, conveniência e controle

AWS KMS oferece diferentes tipos de chaves. Alguns são de propriedade ou gerenciados por AWS, e outros são criados e gerenciados por clientes. Você pode escolher entre essas opções com base no nível de controle que deseja ter sobre as considerações principais e de custo:

- AWS chaves próprias — AWS possui e gerencia essas chaves, e elas são usadas em várias Contas da AWS. Alguns Serviços da AWS oferecem suporte a chaves AWS próprias. Você pode usar essas chaves sem nenhum custo. Esse tipo de chave alivia você do custo e da sobrecarga administrativa de gerenciar o ciclo de vida da chave e do acesso a ela. Para obter mais informações sobre esse tipo de chave, consulte chaves AWS próprias (AWS KMS documentação).
- AWS chaves gerenciadas — Se um AWS service (Serviço da AWS) estiver integrado AWS KMS, ele poderá criar, gerenciar e usar esse tipo de chave em seu nome, a fim de proteger seus recursos nesse serviço. Essas chaves são criadas no seu Conta da AWS e só Serviços da AWS podem ser usadas. Não há taxa mensal para uma chave AWS gerenciada. Eles podem estar sujeitos a taxas de uso além do nível gratuito, mas alguns Serviços da AWS cobrem esses custos para você. Você pode usar políticas de identidade para controlar a visualização e o acesso de auditoria a essas chaves, mas AWS gerencia o ciclo de vida das chaves. Para obter mais informações sobre esse tipo de chave, consulte chaves AWS gerenciadas (AWS KMS documentação). Para obter uma lista abrangente dos Serviços da AWS que se integram com AWS KMS, consulte AWS service (Serviço da AWS) integração (AWS marketing).
- Chaves gerenciadas pelo cliente — Você cria, possui e gerencia esse tipo de chave e tem controle total sobre o ciclo de vida da chave. Para a segregação de tarefas, você pode usar políticas baseadas em identidade e recursos para controlar o acesso à chave. Você também pode configurar a rotação automática de chaves. As chaves gerenciadas pelo cliente incorrem em uma taxa mensal e, se você exceder o nível gratuito, elas também incorrerão em uma taxa pelo uso. Para obter mais informações sobre esse tipo de chave, consulte Chaves gerenciadas pelo cliente (AWS KMS documentação).

Para obter mais informações sobre armazenamento e uso de chaves, consulte AWS Key Management Service preços (AWS marketing).

Tipos de desempenho e criptografia

Com base no tipo de criptografia escolhido nos padrões, você pode usar dois tipos de chaves KMS.

- Simétrico — Todos os AWS KMS key tipos oferecem suporte à criptografia simétrica. Ao criptografar chaves gerenciadas pelo cliente, você pode usar uma chave de força única para criptografia e decodificação com o AES-256-GCM.
- Assimétrico — As chaves gerenciadas pelo cliente oferecem suporte à criptografia assimétrica. Você pode escolher entre diferentes pontos fortes e algoritmos, com base no uso pretendido. As chaves assimétricas podem criptografar e descriptografar com RSA e podem assinar e verificar operações com RSA ou ECC. Os algoritmos de chave assimétrica fornecem inerentemente a separação de funções e simplificam o gerenciamento de chaves. Ao usar criptografia assimétrica com AWS KMS, algumas operações não são suportadas, como rotação de chaves e importação de material de chave externa.

Para obter mais informações sobre as AWS KMS operações suportadas por chaves simétricas e assimétricas, consulte Referência do tipo de chave (AWS KMS documentação).

criptografia envelopada

A criptografia de envelope está incorporada. AWS KMS Em AWS KMS, você gera chaves de dados em formato de texto simples ou criptografado. As chaves de dados criptografadas são criptografadas com uma chave KMS. Você pode armazenar a chave KMS em um armazenamento de chaves personalizado em um AWS CloudHSM cluster. Para obter mais informações sobre os benefícios da criptografia de envelope, consulteSobre a criptografia de envelope.

Local de armazenamento da chave

Você usa políticas para gerenciar o acesso aos AWS KMS recursos. As políticas descrevem quem pode acessar quais recursos. As políticas anexadas a um diretor AWS Identity and Access Management (IAM) são chamadas de políticas baseadas em identidade ou políticas do IAM. As políticas associadas a outros tipos de recursos são chamadas de políticas de recursos. AWS KMS as políticas de recursos para AWS KMS keys são chamadas de políticas principais. Cada chave do KMS tem uma política de chaves.

As políticas de chaves oferecem flexibilidade para armazenar a chave de criptografia em um local central ou armazená-la mais perto dos dados, de forma distribuída. Considere os seguintes AWS KMS recursos ao decidir onde armazenar as chaves KMS no seu: Conta da AWS

- Suporte à infraestrutura de região única — Por padrão, as chaves KMS são específicas da região e nunca saem sem criptografia. AWS KMS Se seus padrões tiverem requisitos rígidos para controlar chaves em uma localização geográfica específica, explore o uso de chaves de região única.
- Suporte à infraestrutura multirregional — AWS KMS também oferece suporte ao tipo de chave para fins especiais denominado chaves multirregionais. Armazenar dados em vários Regiões da AWS é uma configuração comum para recuperação de desastres. Ao usar chaves multirregionais, você pode transferir dados entre regiões sem criptografá-los novamente e gerenciar os dados como se tivesse a mesma chave em cada região. Essa funcionalidade é muito útil se seus padrões exigirem que sua infraestrutura de criptografia abranja várias regiões em uma configuração ativa-ativa. Para obter mais informações, consulte Chaves multirregionais (AWS KMS documentação).
- Gerenciamento centralizado — Se seus padrões exigirem que você armazene as chaves em um local centralizado, você pode usar AWS KMS para armazenar todas as suas chaves de criptografia em uma única. Conta da AWS Você usa políticas de chaves para conceder acesso a outros aplicativos, que podem estar em contas diferentes na mesma região. O gerenciamento centralizado de chaves pode reduzir a sobrecarga administrativa do gerenciamento do ciclo de vida da chave e do controle de acesso à chave.
- Material de chave externa — Você pode importar material de chave gerado externamente para AWS KMS. Support para essa funcionalidade está disponível para chaves simétricas únicas e multirregionais. Como o material da chave simétrica é gerado externamente, você é responsável por proteger os materiais da chave gerada. Para obter mais informações, consulte Material de chave importado (AWS KMS documentação).

Controle de acesso

Em AWS KMS, você pode implementar o controle de acesso em nível granular usando os seguintes mecanismos de política: políticas de chave, políticas de IAM e concessões. Usando esses controles, você pode configurar sua separação de tarefas com base em funções, como administradores, usuários-chave que podem criptografar os dados, usuários-chave que podem descriptografar os dados e usuários-chave que podem criptografar e descriptografar os dados. Para obter mais informações, consulte Autenticação e controle de acesso (AWS KMS documentação).

Auditoria e registro

AWS KMS integra-se com AWS CloudTrail a Amazon EventBridge para fins de registro e monitoramento. Todas as operações AWS KMS da API são registradas e auditáveis em CloudTrail registros. Você pode usar o Amazon CloudWatch, EventBridge, e AWS Lambda para configurar soluções de monitoramento personalizadas para configurar notificações e remediação automática. Para obter mais informações, consulte Registro e monitoramento (AWS KMS documentação).

Perguntas frequentes

Esta seção fornece respostas às perguntas mais comuns ao definir seus padrões de criptografia ou ao criar sua infraestrutura de criptografia na fase de implementação.

Quando eu preciso de criptografia simétrica?

Você pode usar criptografia simétrica quando:

- Velocidade, custo e menor sobrecarga computacional são uma prioridade.
- Você precisa criptografar uma grande quantidade de dados.
- Os dados criptografados não estão saindo dos limites da rede da organização.

Quando eu preciso de criptografia assimétrica?

Você pode usar criptografia assimétrica quando:

- Você precisa compartilhar os dados fora da organização.
- Os regulamentos ou a governança proíbem o compartilhamento da chave.
- O não repúdio é necessário. (O não repúdio impede que um usuário negue compromissos ou ações anteriores.)
- Você precisa separar estritamente o acesso às chaves de criptografia com base nas funções da organização.

Quando eu preciso de criptografia de envelope?

Você precisa oferecer suporte e implementar a criptografia de envelope se sua política de criptografia exigir rotação de chaves. Alguns regimes de governança e conformidade exigem rotação de chaves, ou sua política pode exigir que ela atenda a uma necessidade comercial.

Quando preciso usar um módulo de segurança de hardware (HSM)?

Talvez você precise de um HSM se sua política especificar conformidade com:

- O padrão de criptografia de nível 3 do Federal Information Processing Standards (FIPS) 140-2. Para obter mais informações, consulte Validação FIPS (AWS CloudHSM documentação).
- Padrão do setor APIs, como PKCS #11, Java Cryptography Extension (JCE) ou Microsoft Cryptography API: Next Generation (CNG)

Por que eu deveria gerenciar centralmente as chaves de criptografia?

A seguir estão os benefícios comuns do gerenciamento centralizado de chaves:

- Como as chaves são usadas e administradas em locais diferentes, você pode reutilizá-las, o que pode reduzir custos.
- Você tem mais controle sobre o acesso às chaves de criptografia.
- Armazenar as chaves em um único local facilita a visualização, a auditoria e a atualização das chaves no caso de uma mudança nos padrões.

Preciso usar uma infraestrutura de criptografia específica para dados em repouso?

Sua empresa precisa de uma infraestrutura de criptografia se alguma das seguintes afirmações for verdadeira:

- Sua empresa manipula e armazena dados de qualquer classificação que não seja pública.
- Sua empresa captura e armazena dados sobre funcionários ou clientes.
- Sua empresa lida com dados de PII.
- Sua empresa deve estar em conformidade com regimes regulatórios ou de governança que exigem que os dados sejam criptografados.
- Sua liderança executiva corporativa exigiu a criptografia de todos os dados em repouso.

Como posso AWS KMS ajudar minha organização a atingir seus objetivos de criptografia para dados em repouso?

Além de muitos outros recursos, AWS Key Management Service pode ajudá-lo a:

- Use criptografia de envelope.
- Controle o acesso à chave de criptografia, como separar a administração da chave do uso da chave.
- Compartilhe chaves em vários Regiões da AWS Contas da AWS e.
- Centralize a administração de chaves.
- Automatize e exija a rotação de chaves.

Recursos

AWS service (Serviço da AWS) documentação

- AWS KMS Detalhes criptográficos
- AWS KMS Guia do desenvolvedor
  - Conceitos AWS KMS
  - Chaves para fins especiais
  - Autenticação e controle de acesso para AWS KMS
  - Segurança do AWS KMS
  - Como Serviços da AWS usar AWS KMS
- AWS CloudHSM Guia do usuário

AWS marketing

- AWS KMS preços
- AWS KMS integração com outros Serviços da AWS

AWS Estrutura Well-Architected

- Protegendo dados em trânsito
- Protegendo dados em repouso

Hashing e tokenização

- Como usar a tokenização para melhorar a segurança dos dados e reduzir o escopo da auditoria (AWS postagem no blog)
- Recomendação para aplicativos usando algoritmos de hash aprovados (publicação do NIST)

Vídeos

- Como a criptografia funciona em AWS
- Protegendo seu armazenamento em bloco em AWS
- Atingindo metas de segurança com AWS CloudHSM
- Melhores práticas para implementação AWS Key Management Service
- Um mergulho profundo nos serviços AWS de criptografia

Histórico do documento

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

Alteração	Descrição	Data
Publicação inicial	—	15 de setembro de 2022

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributo.

serviços abstraídos

Veja serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

AGGREGATE FUNCTION

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

AI

Veja inteligência artificial.

AIOps

Veja operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicações

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

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

BCP

Veja planejamento de continuidade de negócios

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

Acesso de emergência

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços 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

Veja AWS Cloud Adoption Framework.

implantação canário

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

CCoE

Veja Centro de Excelência da Nuvem.

CDC

Veja captura de dados de alteração.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja integração e entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas 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 corporativa.

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

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

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog de estratégia Nuvem AWS empresarial. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Veja banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. CI/CD é comumente descrito como um pipeline. CI/CD pode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

data mesh

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Veja linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

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

implantação

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

ambiente de desenvolvimento

Veja ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja recuperação de desastres.

Detecção da oscilação

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

DVSM

Veja mapeamento do fluxo de valor de desenvolvimento.

E

EDA

Veja análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja endpoint de serviço.

serviço de endpoint

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

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

planejamento de recursos empresariais (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja planejamento de recursos empresariais.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

Antecipar-se à falha

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

delimitação de isolamento contra falhas

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

ramificação de recursos

Veja ramificação.

recursos

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

importância do recurso

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

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

transformação de recursos

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

prompt few shot

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

FGAC

Veja controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja modelo de base.

modelo de base (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

golden image

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

estratégia greenfield

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

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais ()OUs. Barreiras de proteção preventivas impõem políticas para

garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja alta disponibilidade.

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas 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 hold-out

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de machine learning. Você pode usar dados de hold-out para avaliar a performance do modelo comparando as predições do modelo com os dados de retenção.

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

eu

IaC

Veja 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 Internet das Coisas Industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das coisas (IoT)

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

interpretabilidade

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

IoT

Veja Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Veja biblioteca de informações de TI.

ITSM

Veja gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

grande modelo de linguagem (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulo.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

LLM

Veja grande modelo de linguagem.

ambientes inferiores

Veja ambiente.

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte Machine learning.

ramificação principal

Veja ramificação.

Malware

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

Serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Veja Programa de Aceleração da Migração.

mecanismo

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

conta de membro

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

MES

Veja sistema de execução de manufatura.

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio

de uma interface bem definida usando leveza. APIs Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte Implementação de microsserviços em. AWS

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja machine learning.

modernização

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

avaliação de preparação para modernização

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

aplicações monolíticas (monólitos)

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

MPA

Veja Avaliação do Portfólio para Migração.

MQTT

Veja Transporte de Telemetria de Enfileiramento de Mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja controle de acesso de origem.

OAI

Veja identidade de acesso de origem.

OCM

Veja gerenciamento de alterações organizacionais.

migração offline

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

OI

Veja integração de operações.

Ola

Veja acordo de nível operacional.

migração online

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

OPC-UA

Veja Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (TO)

Sistemas de hardware e software que trabalham com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas de

tecnologia da informação (TI) e tecnologia operacional (TO) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

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

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de 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 análise de prontidão operacional.

OT

Veja tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja informações de identificação pessoal.

manual

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

PLC

Veja controlador lógico programável.

PLM

Veja gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pushdown de predicados

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

controle preventivo

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

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais

informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja ambiente.

controlador lógico programável (PLC)

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

encadeamento de prompts

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

pseudonimização

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

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

RAG

Veja geração aumentada via recuperação.

ransomware

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

Matriz RASCI

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

RCAC

Veja controle de acesso por linha e coluna.

réplica de leitura

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

Redefinir arquitetura

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

Retirada

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja objetivo de ponto de recuperação.

RTO

Veja objetivo de tempo de recuperação.

runbook

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

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login Console de gerenciamento da AWS ou chamar as operações da AWS API sem que você precise criar um usuário no IAM

para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja política de controle de serviço.

secret

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

segurança desde a concepção

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

controle de segurança

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

hardening da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja sistema de gerenciamento de eventos e informações de segurança.

ponto único de falha (SPOF)

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

SLA

Veja cacordo de serviço.

SLI

Veja indicador de nível de serviço.

SLO

Veja objetivo de nível de serviço.

split-and-seed modelo

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

SPOF

Veja ponto único de falha.

esquema em estrela

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

padrão strangler fig

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

sub-rede

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

controle supervisório e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja ambiente.

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

WORM

Veja gravação única e várias leituras.

WQF

Veja AWS Workload Qualification Framework.

gravação única e várias leituras (WORM)

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

Z

exploração de dia zero

Um ataque, normalmente malware, que tira proveito de uma vulnerabilidade zero-day.

vulnerabilidade de dia zero

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

prompt zero shot

Fornecer a um LLM instruções para realizar uma tarefa, mas sem exemplos (shots) que possam ajudar a orientá-lo. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt. Veja também prompts few-shot.

aplicação zumbi

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

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