Melhores práticas e recursos de criptografia para Serviços da AWS

AWS Orientação prescritiva

AWS Orientação prescritiva: Melhores práticas e recursos de criptografia para Serviços da AWS

Table of Contents

Práticas recomendadas e recursos de criptografia dos Serviços da AWS

Kurt Kumar, Amazon Web Services (AWS)

Dezembro de 2022 (histórico do documento)

As ameaças modernas de segurança cibernética incluem o risco de uma violação de dados, o que ocorre quando uma pessoa autorizada obtém acesso à sua rede e rouba os dados da empresa. Os dados são um ativo comercial exclusivo de cada organização. Eles podem incluir informações do cliente, planos de negócios, documentos de design ou código. Proteger a empresa significa proteger seus dados.

Medidas como firewalls podem ajudar a evitar a ocorrência de uma violação de dados. No entanto, a criptografia de dados pode ajudar a proteger os dados da sua empresa mesmo após a ocorrência de uma violação. Ela fornece outra camada de defesa contra divulgação não intencional dos dados. Para acessar dados criptografados na Nuvem AWS, os usuários precisam de permissões para usar a chave para descriptografar e precisam de permissões para usar o serviço em que os dados residem. Sem essas duas permissões, os usuários não conseguem descriptografar e visualizar os dados.

Geralmente, há dois tipos de dados que você pode criptografar. 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. Os exemplos incluem armazenamento em blocos, armazenamento de objetos, bancos de dados, arquivos e dispositivos de Internet das Coisas (IoT). Este guia discute considerações e práticas recomendadas para criptografar os dois tipos de dados. Ele também analisa os recursos e controles de criptografia disponíveis em muitos Serviços da AWS para que você possa implementar essas recomendações de criptografia no nível de serviço em seus ambientes de Nuvem AWS.

Público-alvo

Este guia pode ser usado por organizações de pequeno, médio e grande porte nos setores público e privado. Se sua organização está nos estágios iniciais de avaliação e implementação de uma estratégia de proteção de dados ou tem como objetivo aprimorar os controles de segurança existentes, as recomendações descritas neste guia são mais adequadas para os seguintes públicos:

- Líderes executivos que formulam políticas para suas empresas, como diretores executivos (CEOs), 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
- Partes envolvidas da empresa e proprietários de aplicações que são responsáveis por:
  - Avaliação da postura de risco, classificação de dados e requisitos de proteção
  - Monitoramento da conformidade com padrões organizacionais estabelecidos
- Diretores de conformidade, auditoria interna e governança encarregados de monitorar a adesão às políticas de conformidade, incluindo regimes de conformidade estatutários e voluntários

Sobre os serviços de criptografia da AWS

Um algoritmo de criptografia é uma fórmula ou procedimento que converte uma mensagem de texto simples em um texto cifrado criptografado. Se você não tiver experiência com criptografia ou com sua terminologia, recomendamos ler Sobre criptografia de dados e Conceitos da criptografia antes de continuar com este guia.

Os serviços de criptografia da AWS dependem de algoritmos de criptografia seguros e de código aberto. Esses algoritmos são examinados por órgãos públicos de padrões e por pesquisas acadêmicas. Alguns serviços e ferramentas da AWS impõem o uso de um algoritmo específico. Em outros serviços, é possível escolher entre vários algoritmos e comprimentos de chave disponíveis ou usar os padrões recomendados.

Esta seção descreve alguns dos algoritmos compatíveis com serviços e ferramentas da AWS. A criptografia pode ser dividida em duas categorias, simétrica e assimétrica, com base no funcionamento de suas chaves:

- A criptografia simétrica usa a mesma chave para criptografar e descriptografar os dados. Os Serviços da AWSsão compatíveis com o Advanced Encryption Standard (AES) e o Triple Data Encryption Standard (3DES ou TDES), que são dois algoritmos simétricos amplamente usados. Para obter mais informações, consulte Algoritmos simétricos no Guia de ferramentas e serviços criptográficos da AWS.
- A criptografia simétrica usa um par de chaves: uma chave pública para criptografia e uma chave privada para descriptografia. A chave pública pode ser compartilhada porque ela não é usada para descriptografia, mas o acesso à chave privada deve ser altamente restrito. Os Serviços da AWS normalmente são compatíveis com os algoritmos assimétricos RSA e criptografia de curva elíptica (ECC). Para obter mais informações, consulte Algoritmos assimétricos no Guia de ferramentas e serviços criptográficos da AWS.

Os serviços criptográficos da AWS estão em conformidade com uma ampla variedade de padrões de segurança criptográfica para que você possa cumprir regulamentações governamentais ou profissionais. Para obter uma lista completa dos padrões da segurança de dados seguidos pela Serviços da AWS, consulte Programas de conformidade da AWS Para obter mais informações sobre ferramentas e serviços criptográficos, consulte Ferramentas e serviços criptográficas da AWS.

Práticas recomendadas gerais de criptografia

Esta seção fornece recomendações que se aplicam ao criptografar dados na Nuvem AWS. Essas práticas recomendadas gerais de criptografia não são específicas para os Serviços da AWS. Esta seção inclui os seguintes tópicos:

- Classificação de dados
- Criptografia de dados em trânsito
- Criptografia de dados em repouso

Classificação de dados

Classificação de dados é 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. As categorias podem incluir altamente confidenciais, confidenciais, não confidenciais e públicos, mas os níveis de classificação e seus nomes podem variar de organização para organização. Para obter mais informações sobre o processo, as considerações e os modelos de classificação de dados, consulte Classificação de dados (whitepaper da AWS).

Após classificar seus dados, você poderá criar uma estratégia de criptografia para sua organização com base no nível de proteção necessário para cada categoria. Por exemplo, sua organização pode decidir que dados altamente confidenciais devem usar criptografia assimétrica e que dados públicos não precisam de criptografia. Para obter mais informações sobre como criar uma estratégia de criptografia, consulte Criar uma estratégia de criptografia corporativa para dados em repouso. Embora as considerações e recomendações técnicas desse guia sejam específicas para dados em repouso, também é possível usar a abordagem em fases para criar uma estratégia de criptografia para dados em trânsito.

Criptografia de dados em trânsito

Todos os dados transmitidos entre Regiões da AWS por meio da rede global da AWS são automaticamente criptografados na camada física antes de sair das instalações seguras da AWS. Todo o tráfego entre as zonas de disponibilidade é criptografado.

Práticas recomendadas gerais ao criptografar dados em trânsito na Nuvem AWS são:

- Defina uma política de criptografia organizacional para dados em trânsito com base em sua classificação de dados, requisitos organizacionais e quaisquer padrões regulatórios ou de conformidade aplicáveis. É altamente recomendável criptografar dados em trânsito classificados como altamente confidenciais ou confidenciais. Sua política também pode especificar criptografia para outras categorias, como dados públicos ou não confidenciais, conforme necessário.
- Ao criptografar dados em trânsito, recomendamos usar algoritmos de criptografia aprovados, modos de criptografia de blocos e comprimentos de chave, conforme definido em sua política de criptografia.
- Criptografe o tráfego entre ativos de informação e sistemas dentro da rede corporativa e infraestrutura da Nuvem AWS usando uma das seguintes opções:
  - Conexões do AWS Site-to-Site VPN
  - Uma combinação de conexões do AWS Site-to-Site VPN e do AWS Direct Connect que fornece uma conexão privada criptografada por IPsec
  - Conexões do AWS Direct Connect que oferecem suporte ao MAC Security (MACsec) para criptografar dados de redes corporativas na localização da Amazon VPC
- 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. Para obter mais informações sobre como aplicar permissões de privilégios mínimos, consulte Práticas recomendadas de segurança no IAM e Práticas recomendadas para políticas do IAM.

Criptografia de dados em repouso

Todos os serviços de armazenamento de dados da AWS, como o Amazon Simple Storage Service (Amazon S3) e o Amazon Elastic File System (Amazon EFS), oferecem opções para criptografar dados em repouso. A criptografia é realizada usando a cifra de bloco Advanced Encryption Standard (AES-256) de 256 bits e serviços de criptografia da AWS, como o AWS Key Management Service (AWS KMS) ou o AWS CloudHSM.

Você pode criptografar dados usando criptografia do lado do cliente ou criptografia do lado do servidor, com base em fatores como classificação de dados, necessidade de end-to-end criptografia ou limitações técnicas que impedem o uso da criptografia: end-to-end

- Criptografia do lado do cliente é o ato de criptografar dados localmente antes que a aplicação ou o serviço de destino os receba. O serviço AWS service (Serviço da AWS) recebe os dados criptografados. Ele não atua na criptografia ou descriptografia desses dados. Na criptografia do lado do cliente, é possível pode usar o AWS KMS, o AWS Encryption SDK ou outras ferramentas ou serviços de criptografia de terceiros.
- A criptografia do lado do servidor é o ato de criptografar dados em seu destino pela aplicação ou serviço que os recebe. Na criptografia do lado do servidor, é possível usar o AWS KMS para criptografar todo o bloco de armazenamento. Você também pode usar outras ferramentas ou serviços de criptografia de terceiros, como o LUKS para criptografar um sistema de arquivos Linux no nível do sistema operacional (SO).

As práticas recomendadas gerais para criptografar dados em repouso na Nuvem AWS são:

- Defina uma política de criptografia organizacional para dados em repouso com base em sua classificação de dados, requisitos organizacionais e quaisquer padrões regulatórios ou de conformidade aplicáveis. Para obter mais informações, consulte Criar uma estratégia de criptografia corporativa para dados em repouso. É altamente recomendável criptografar dados em repouso classificados como altamente confidenciais ou confidenciais. Sua política também pode especificar criptografia para outras categorias, como dados públicos ou não confidenciais, conforme necessário.
- Ao criptografar dados em repouso, recomendamos usar algoritmos de criptografia aprovados, modos de criptografia de blocos e comprimentos de chave.
- Identifique políticas de controle de acesso para suas chaves de criptografia com base no princípio de privilégio mínimo.

Práticas recomendadas de criptografia para Serviços da AWS

Esta seção inclui as melhores práticas e recomendações específicas Serviços da AWS. Esta seção discute os seguintes serviços:

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (Amazon EC2) e Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (Amazon RDS)
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

AWS CloudTrail

O AWS CloudTrail ajuda a habilitar governança, conformidade e auditorias operacionais e de risco da sua Conta da AWS.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- CloudTrail os registros devem ser criptografados usando um sistema gerenciado pelo cliente AWS KMS key. Escolha uma chave do KMS que esteja na mesma região que o bucket do S3 que recebe seus arquivos de log. Para obter mais informações, consulte Atualizar uma trilha para usar sua chave do KMS.

- Como uma camada de segurança adicional, habilite a validação do arquivo de log para trilhas. Isso ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Para obter instruções, consulte Habilitando a validação da integridade do arquivo de log para CloudTrail.
- Use endpoints de VPC de interface para permitir CloudTrail a comunicação com recursos em outras VPCs sem atravessar a Internet pública. Para obter mais informações, consulte Usar a AWS CloudTrail com endpoints da VPC de interface.
- Adicione uma chave de `aws:SourceArn` condição à política de chaves do KMS para garantir que a chave do KMS seja CloudTrail usada somente para uma trilha ou trilhas específicas. Para obter mais informações, consulte Configurar AWS KMS key políticas para CloudTrail.
- Em AWS Config, implemente a regra cloud-trail-encryption-enabled AWS gerenciada para validar e aplicar a criptografia do arquivo de log.
- Se CloudTrail estiver configurado para enviar notificações por meio de tópicos do Amazon Simple Notification Service (Amazon SNS), adicione `aws:SourceArn` uma chave de condição (ou `aws:SourceAccount` opcionalmente) à declaração de política para impedir CloudTrail o acesso não autorizado da conta ao tópico do SNS. Para obter mais informações, consulte a política de tópicos do Amazon SNS para. CloudTrail
- Se você estiver usando AWS Organizations, crie uma trilha da organização que registre todos os Contas da AWS eventos dessa organização. Isso inclui a conta de gerenciamento e todas as contas-membros na organização. Para obter mais informações, consulte Criar uma trilha para uma organização.
- Crie uma trilha que se aplique a todos os Regiões da AWS locais em que você armazena dados corporativos, para registrar a Conta da AWS atividade nessas regiões. Quando AWS inicia uma nova região, inclui CloudTrail automaticamente a nova região e registra eventos nessa região.

Amazon DynamoDB

O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece performance rápida, previsível e escalável. A criptografia em repouso do DynamoDB protege os dados em uma tabela criptografada, incluindo a chave primária, os índices secundários local e global, os fluxos, as tabelas globais, os backups e os clusters do DynamoDB Accelerator (DAX) sempre que os dados são armazenados em mídia durável.

De acordo com os requisitos de classificação de dados, a confidencialidade e a integridade dos dados podem ser mantidas implementando a criptografia do lado do servidor ou do lado do cliente:

Para criptografia do lado do servidor, ao criar uma nova tabela, você pode usar o AWS KMS keys para criptografar a tabela. Você pode usar chaves AWS próprias, chaves AWS gerenciadas ou chaves gerenciadas pelo cliente. Recomendamos usar chaves gerenciadas pelo cliente porque sua organização tem controle total da chave e porque, quando você usa esse tipo de chave, a chave de criptografia em nível de tabela, a tabela, os índices secundários local e global e os fluxos do DynamoDB são criptografados com a mesma chave. Para obter mais informações sobre esses tipos de chave, consulte Chaves e AWS chaves do cliente.

> **Note**
>
> Você pode alternar entre uma AWS chave própria, uma chave AWS gerenciada e uma chave gerenciada pelo cliente a qualquer momento.

Para criptografia do lado do cliente e end-to-end proteção de dados, tanto em repouso quanto em trânsito, você pode usar o Amazon DynamoDB Encryption Client. Além da criptografia, que protege a confidencialidade do valor do atributo do item, o DynamoDB Encryption Client assina o item. Ele fornece proteção de integridade habilitando a detecção de alterações não autorizadas no item, incluindo a adição ou a exclusão de atributos ou a substituição de um valor criptografado por outro.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Limite as permissões para desabilitar ou programar a exclusão da chave somente para quem realmente precisa realizar essas tarefas. Esses estados impedem que todos os usuários e o serviço DynamoDB possam criptografar ou descriptografar dados e realizar operações de leitura e gravação~na tabela.
- Embora o DynamoDB criptografe dados em trânsito usando HTTPS por padrão, controles de segurança adicionais são recomendados. Você pode usar qualquer uma das opções a seguir:
  - AWS Site-to-Site VPN conexão usando IPsec para criptografia.
  - AWS Direct Connect conexão para estabelecer uma conexão privada.
  - AWS Direct Connect conexão com AWS Site-to-Site VPN conexão para uma conexão privada criptografada por IPsec.
  - Se o acesso ao DynamoDB for necessário apenas por meio de uma nuvem privada virtual (VPC), use um endpoint de gateway da VPC e permita acesso somente pelos recursos dentro da VPC. Isso evita que o tráfego atravesse a Internet pública.
- Se você estiver usando endpoints da VPC, restrinja as políticas de endpoint e as políticas do IAM associadas ao endpoint somente a usuários, recursos e serviços autorizados. Para obter mais

informações, consulte Controlar o acesso a endpoints do DynamoDB usando políticas do IAM e Controlar o acesso a serviços usando políticas de endpoint.

- Você pode implementar a criptografia de dados em nível de coluna no nível de aplicação para dados que exigem criptografia, de acordo com sua política de criptografia.
- Configure clusters DAX para criptografar dados em repouso, como dados em cache, dados de configuração e arquivos de log, no momento da configuração do cluster. Não é possível ativar a criptografia em repouso em um cluster existente. Essa criptografia do lado do servidor ajuda a proteger os dados contra acesso não autorizado por meio do armazenamento subjacente. A criptografia DAX em repouso se integra automaticamente AWS KMS para gerenciar a chave padrão de serviço único usada para criptografar os clusters. Se uma chave padrão de serviço não existir quando um cluster DAX criptografado for criado, AWS KMS criará automaticamente uma nova chave AWS gerenciada. Para obter mais informações, consulte Criptografia de DAX em repouso.

  > **Note**
  >
  > Não é possível usar chaves gerenciadas pelo cliente com clusters do DAX.

- Configure clusters DAX para criptografar dados em trânsito no momento da configuração do cluster. Não é possível ativar a criptografia em trânsito em um cluster existente. O DAX usa TLS para criptografar as solicitações e as respostas entre a aplicação e o cluster e usa o certificado x509 do cluster para autenticar a identidade do cluster. Para obter mais informações, consulte Criptografia do DAX em trânsito.
- Em AWS Config, implemente a regra dax-encryption-enabled AWS gerenciada para validar e manter a criptografia dos clusters DAX.

Amazon Elastic Compute Cloud e Amazon Elastic Block Store

O Amazon Elastic Compute Cloud (Amazon EC2) oferece capacidade de computação escalável na Nuvem AWS. Você pode iniciar quantos servidores virtuais precisar e escalá-los na vertical rapidamente. O Amazon Elastic Block Store (Amazon EBS) oferece volumes de armazenamento em bloco para usar com instâncias do EC2.

Considere as seguintes práticas recomendadas de criptografia para esses serviços:

- Marque todos os volumes do EBS com a chave e o valor de classificação de dados apropriados. Isso ajuda você a determinar e implementar os requisitos adequados de segurança e criptografia de acordo com suas políticas.
- De acordo com sua política de criptografia e a viabilidade técnica, configure a criptografia para dados em trânsito entre instâncias do EC2 ou entre instâncias do EC2 e sua rede on-premises.
- Criptografe os volumes do EBS de dados e inicialização de uma instância do EC2. Um volume do EBS criptografado protege os seguintes dados:
  - Dados em repouso dentro do volume
  - Todos os dados que são movidos entre o volume e a instância
  - Todos os snapshots criados a partir do volume
  - Todos os volumes criados a partir desses snapshots

Para obter mais informações, consulte Como a criptografia do EBS funciona.

- Habilite a criptografia para volumes do EBS por padrão para sua conta na região atual. Isso aplica a criptografia de quaisquer novos volumes e cópias de snapshot do EBS. Não há efeito sobre volumes ou snapshots do EBS existentes. Para obter mais informações, consulte Criptografia padrão.
- Criptografe o volume raiz do armazenamento de instâncias para uma instância do Amazon EC2. Isso ajuda a proteger arquivos de configuração e dados armazenados com o sistema operacional. Para obter mais informações, consulte Como proteger dados em repouso com a criptografia de armazenamento de instâncias do Amazon EC2 (AWS postagem no blog)
- Em AWS Config, implemente a regra de volumes criptografados em verificações automatizadas que validam e impõem as configurações de criptografia apropriadas.

Amazon Elastic Container Registry

O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado de registro de imagens de contêineres seguro, escalável e confiável.

O Amazon ECR armazena imagens em buckets do Amazon S3 gerenciados pelo Amazon ECR. Cada repositório do Amazon ECR tem uma configuração de criptografia, que é definida quando o repositório é criado. Por padrão, o Amazon ECR usar criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) Para obter mais informações, consulte Criptografia em repouso (documentação do Amazon ECR).

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Em vez de usar a criptografia do lado do servidor padrão com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3), use chaves do KMS gerenciadas pelo cliente armazenadas no AWS KMS. Esse tipo de chave fornece as opções de controle mais granulares.

  > **Note**
  >
  > A chave KMS deve existir da mesma forma que Região da AWS o repositório.

- Não revogue as concessões que o Amazon ECR cria por padrão quando você provisiona um repositório. Isso pode afetar a funcionalidade, como acessar dados, criptografar novas imagens enviadas ao repositório ou descriptografá-las ao serem extraídas.
- Use AWS CloudTrail para registrar as solicitações para as quais o Amazon ECR envia. AWS KMS As entradas no log contêm uma chave de contexto de criptografia para facilitar a identificação.
- Configure políticas do Amazon SQS para controlar o acesso de endpoints da Amazon VPC ou de VPCs específicas. Efetivamente, isso isola o acesso via rede a um determinado recurso do Amazon ECR, permitindo o acesso somente por meio da VPC específica. Ao estabelecer uma conexão de rede privada virtual (VPN) com um endpoint da Amazon VPC, é possível criptografar os dados em trânsito.
- O Amazon ECR oferece suporte a políticas baseadas em recursos. Usando essas políticas, você pode restringir o acesso com base no endereço IP de origem ou no endereço IP específico. AWS service (Serviço da AWS)

Amazon Elastic Container Service

O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres escalável e rápido que facilita a execução, a interrupção e o gerenciamento de contêineres em um cluster.

Com o Amazon ECS, é possível criptografar dados em trânsito usando qualquer uma das seguintes abordagens:

- Crie uma malha de serviços Usando AWS App Mesh, configure conexões TLS entre os proxies Envoy implantados e os endpoints de malha, como nós virtuais ou gateways virtuais. Você pode usar certificados TLS de AWS Private Certificate Authority ou certificados fornecidos pelo cliente. Para obter mais informações e orientações, consulte Habilitar a criptografia de tráfego entre

serviços em AWS App Mesh uso AWS Certificate Manager (ACM) ou certificados fornecidos pelo cliente (postagem do blog).AWS

- Se houver suporte, use AWS Nitro Enclaves. AWS O Nitro Enclaves é um recurso do Amazon EC2 que permite criar ambientes de execução isolados, chamados enclaves, a partir de instâncias do Amazon EC2. Eles foram projetados para ajudar a proteger seus dados mais sensíveis. Além disso, o ACM para Nitro Enclaves permite a você usar certificados SSL/TLS públicos e privados com suas aplicações Web e servidores em execução em instâncias do Amazon EC2 com o AWS Nitro Enclaves. Para obter mais informações, consulte AWS Nitro Enclaves — Ambientes EC2 isolados para processar dados confidenciais (AWS postagem no blog).
- Use o protocolo Server Name Indication (SNI) com o Application Load Balancer. É possível implantar várias aplicações em um único listener HTTPS para um Application Load Balancer. Cada receptor tem seu próprio certificado TLS. É possível usar certificados fornecidos pelo ACM ou certificados autoassinados. Tanto o Application Load Balancer quanto o Network Load Balancer são compatíveis com o SNI. Para obter mais informações, consulte Application Load Balancers Now Support Multiple TLS Certificates with Smart Selection Using SNI (AWS postagem no blog).
- Para maior segurança e flexibilidade, use AWS Private Certificate Authority para implantar um certificado TLS com a tarefa do Amazon ECS. Para obter mais informações, consulte Mantendo o TLS até o contêiner, parte 2: Usando CA privada da AWS (postagem AWS do blog).
- Implemente TLS mútuo (mTLS) no App Mesh usando o serviço de descoberta secreta (Envoy) ou certificados hospedados no ACM (). GitHub

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Quando tecnicamente viável, para maior segurança, configure Endpoints da VPC de interface do Amazon ECS em AWS PrivateLink. O acesso a esses endpoints por meio de uma conexão VPN criptografa os dados em trânsito.
- Armazene materiais confidenciais, como chaves de API ou credenciais de banco de dados, em segurança. É possível armazená-los como parâmetros criptografados no Parameter Store, um recurso do AWS Systems Manager. No entanto, recomendamos que você use AWS Secrets Manager porque esse serviço permite alternar segredos automaticamente, gerar segredos aleatórios e compartilhar segredos entre Contas da AWS:
- Para ajudar a reduzir o risco de vazamento de dados de variáveis de ambiente, recomendamos que você use o driver CSI e AWS Secrets Manager Config Provider for Secret Store (). GitHub Esse driver permite que os segredos armazenados no Secrets Manager e os parâmetros armazenados no Parameter Store apareçam como arquivos montados em pods do Kubernetes.

> **Note**
>
> AWS Fargate não é suportado.

- Se usuários ou aplicativos em seu data center ou terceiros externos na Web estiverem fazendo solicitações diretas da API HTTPS Serviços da AWS, assine essas solicitações com credenciais de segurança temporárias obtidas de AWS Security Token Service (AWS STS).

Amazon Elastic File System

Amazon Elastic File System (Amazon EFS) ajuda você a criar e configurar sistemas de arquivos compartilhados na Nuvem AWS.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Em AWS Config, implemente a regra efs-encrypted-check AWS gerenciada. Essa regra verifica se o Amazon EFS está configurado para criptografar os dados do arquivo usando AWS KMS.
- Imponha a criptografia aos sistemas de arquivos do Amazon EFS criando um CloudWatch alarme da Amazon que monitora CloudTrail os registros de `CreateFileSystem` eventos e aciona um alarme se um sistema de arquivos não criptografado for criado. Para obter mais informações, consulte Passo a passo: aplicar criptografia em um sistema de arquivos do Amazon EFS em repouso.
- Monte o sistema de arquivos usando o assistente de montagem do EFS. Isso configura e mantém um túnel TLS 1.2 entre o cliente e o serviço Amazon EFS e roteia todo o tráfego de Network File System (NFS) por esse túnel criptografado. O comando a seguir implementa o uso do TLS para criptografia em trânsito.

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  Para obter mais informações, consulte Usar o assistente de montagem do EFS para montar sistemas de arquivos do EFS.
- Usando AWS PrivateLink e implementando endpoints VPC de interface para estabelecer uma conexão privada entre VPCs e a API do Amazon EFS. Os dados em trânsito pela conexão VPN de e para o endpoint são criptografados. Para obter mais informações, consulte Acessar um AWS service (Serviço da AWS) usando um endpoint da VPC de interface.

- Use a chave de condição `elasticfilesystem:Encrypted` nas políticas baseadas em identidade do IAM para impedir que os usuários criem sistemas de arquivos do EFS que não sejam criptografados. Para obter mais informações, consulte Usar o IAM para forçar a criação de sistemas de arquivos criptografados.
- As chaves do KMS usadas para criptografia do EFS devem ser configuradas para acesso com privilégios mínimos usando políticas de chaves baseadas em recursos.
- Use a chave de condição `aws:SecureTransport` na política do sistema de arquivos do EFS para forçar o uso de TLS para clientes NFS ao conectar a um sistema de arquivos do EFS. Para obter mais informações, consulte Criptografia de dados em trânsito em Criptografando dados de arquivos com o Amazon Elastic File System (AWS Whitepaper).

Amazon Elastic Kubernetes Service

O Amazon Elastic Kubernetes Service (Amazon EKS) ajuda você a executar o AWS Kubernetes sem precisar instalar ou manter seu próprio plano de controle ou nós do Kubernetes. No Kubernetes, os segredos ajudam você a gerenciar informações confidenciais, como certificados de usuário, senhas ou chaves de API. Por padrão, esses segredos são armazenados sem criptografia no armazenamento de dados subjacente do servidor da API, o etcd. Qualquer usuário com acesso à API ou ao `etcd` pode recuperar ou modificar um segredo. Além disso, qualquer pessoa autorizada a criar um pod em um namespace pode usar esse acesso para ler qualquer segredo nesse namespace. Você pode criptografar esses segredos em repouso no Amazon EKS usando AWS KMS keys chaves gerenciadas ou chaves AWS gerenciadas pelo cliente. Uma abordagem alternativa de uso `etcd` é usar o AWS Secrets and Config Provider (ASCP) (GitHub repositório). O ASCP se integra ao IAM e a políticas com base em recursos para limitar e restringir o acesso a segredos somente em pods específicos do Kubernetes em um cluster.

Você pode usar os seguintes serviços AWS de armazenamento com o Kubernetes:

- Para o Amazon Elastic Block Store (Amazon EBS), é possível usar o driver de armazenamento em árvore ou o Driver da CSI do Amazon EBS. Ambos incluem parâmetros para criptografar volumes e fornecer uma chave gerenciada pelo cliente.
- Para o Amazon Elastic File System (Amazon EFS), é possível usar o Driver da CSI do Amazon EFS compatível com provisionamento dinâmico e estático.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Para o Amazon EFS, configure a criptografia em trânsito adicionando o parâmetro `tls` a `mountOptions` no volume persistente do Amazon EKS. Para obter mais informações, consulte Criptografia de dados e gerenciamento de segredos (Guia de práticas recomendadas do Amazon EKS).
- Se você estiver usando o `etcd`, que armazena objetos secretos não criptografados por padrão, faça o seguinte para ajudar a protegê-los:
  - Criptografia de dados em repouso secretos (documentação do Kubernetes).
  - Ative ou configure a autorização por meio de regras de controle de acesso baseado em perfil (RBAC) que restringem a leitura e a gravação do segredo. Restrinja as permissões para criar novos segredos ou substituir segredos existentes. Para obter mais informações, consulte Visão geral da autorização (documentação do Kubernetes).
  - Se você estiver definindo vários contêineres em um pod e somente um desses contêineres precisar acessar um segredo, defina a montagem do volume para que os outros contêineres não tenham acesso a esse segredo. Segredos montados como volumes são instanciados como volumes `tmpfs` e são removidos automaticamente do nó quando o pod é excluído. Também é possível usar variáveis de ambiente, mas não recomendamos essa abordagem porque os valores das variáveis de ambiente podem aparecer nos registros. Para obter mais informações, consulte Segredos (documentação do Kubernetes).
  - Quando possível, evite conceder acesso a solicitações `watch` e `list` para segredos em um namespace. Na API do Kubernetes, essas solicitações são poderosas porque permitem que o cliente inspecione os valores de cada segredo nesse namespace.
  - Permita que somente os administradores de cluster acessem o `etcd`, incluindo acesso somente leitura.
  - Se houver várias instâncias do `etcd`, garanta que `etcd` use TLS para comunicação entre pares `etcd`.
- Se você estiver usando o ASCP, faça o seguinte para ajudar a proteger os segredos:
  - Use Perfis do IAM para contas de serviço para limitar o acesso secreto somente a pods autorizados.
  - Ative a criptografia de segredos do Kubernetes usando o Provedor de Criptografia (GitHub repositório) para implementar a AWS criptografia de envelope com uma chave KMS gerenciada pelo cliente.
- Crie um filtro de CloudWatch métricas e um alarme da Amazon para enviar alertas para operações especificadas pelo administrador, como exclusão secreta ou uso de uma versão secreta no

período de espera para ser excluída. Para obter mais informações, consulte Criar um alarme com base na detecção de anomalias.

AWS Encryption SDK

O AWS Encryption SDK é uma biblioteca de criptografia do lado do cliente com código aberto. Ele usa os padrões do setor e as melhores práticas para apoiar a implementação e a interoperabilidade em várias linguagens de programação. AWS Encryption SDK criptografa dados usando um algoritmo de chave simétrica seguro, autenticado e oferece uma implementação padrão que segue as melhores práticas de criptografia. Para obter mais informações, consulte Pacotes de algoritmos compatíveis no AWS Encryption SDK.

Considere as seguintes práticas recomendadas para esse serviço:

- Siga todas as recomendações em Práticas recomendadas para o AWS Encryption SDK.
- Selecione uma ou mais chaves de empacotamento para ajudar a proteger suas chaves de dados. Para obter mais informações, consulte Selecionar chaves de empacotamento.
- Passe o `KeyId` parâmetro para a ReEncryptoperação para ajudar a evitar o uso de uma chave KMS não confiável. Para obter mais informações, consulte Criptografia aprimorada do lado do cliente: compromisso explícito KeyIds e fundamental (AWS postagem no blog).
- Ao usar AWS Encryption SDK com AWS KMS, use a `KeyId` filtragem local. Para obter mais informações, consulte Criptografia aprimorada do lado do cliente: compromisso explícito KeyIds e fundamental (AWS postagem no blog).
- Para aplicativos com grandes volumes de tráfego que exigem criptografia ou descriptografia, ou se sua conta estiver excedendo as cotas de AWS KMS solicitação, você pode usar o recurso de armazenamento em cache da chave de dados do. AWS Encryption SDK Observe as seguintes práticas recomendadas para o armazenamento em cache de chaves de dados:
  - Configure limites de segurança de cache para limitar duração do uso de cada chave de dados e quantos dados são protegidos em cada chave de dados. Para obter recomendações ao configurar esses limites, consulte Definir limites de segurança de cache.
  - Limite o cache local ao menor número de chaves de dados necessárias para obter melhorias de performance para seu caso de uso específico de aplicação. Para obter instruções e um exemplo de configuração de limites para o cache local, consulte Usando o cache de chaves de dados: S. tep-by-step

Para obter mais informações, consulte AWS Encryption SDK: Como decidir se o armazenamento em cache de chaves de dados é adequado para seu aplicativo (postagem AWS no blog).

AWS Key Management Service

AWS Key Management Service (AWS KMS) ajuda você a criar e controlar chaves criptográficas para ajudar a proteger seus dados. AWS KMS se integra com a maioria dos outros Serviços da AWS que podem criptografar seus dados. Para obter uma lista completa, consulte Serviços da AWS integrado com AWS KMS. AWS KMS também se integra AWS CloudTrail para registrar o uso de suas chaves KMS para necessidades de auditoria, regulamentação e conformidade.

As chaves KMS são o principal recurso e são representações lógicas de uma chave criptográfica. AWS KMS Há três tipos principais de chaves do KMS:

- As chaves gerenciadas pelo cliente são chaves do KMS criadas por você.
- AWS chaves gerenciadas são chaves KMS Serviços da AWS criadas em sua conta, em seu nome.
- AWS chaves próprias são chaves KMS que um AWS service (Serviço da AWS) possui e gerencia, para uso em várias Contas da AWS.

Para obter mais informações sobre esses tipos de chave, consulte Chaves do cliente e chaves da AWS.

No Nuvem AWS, as políticas são usadas para controlar quem pode acessar recursos e serviços. Por exemplo, no AWS Identity and Access Management (IAM), as políticas baseadas em identidade definem permissões para usuários, grupos de usuários ou funções, e as políticas baseadas em recursos são anexadas a um recurso, como um bucket do S3, e definem quais diretores têm acesso permitido, ações suportadas e quaisquer outras condições que devem ser atendidas. Semelhante às políticas do IAM, AWS KMS usa políticas de chaves para controlar o acesso a uma chave KMS. Cada chave do KMS deve ter uma política de chave, e cada chave pode ter apenas uma política de chave. Observe o seguinte ao definir políticas que permitem ou negam acesso a chaves do KMS:

- Você pode controlar a política de chaves para chaves gerenciadas pelo cliente, mas não pode controlar diretamente a política de chaves para chaves AWS gerenciadas ou para chaves AWS próprias.
- As principais políticas permitem conceder acesso granular às chamadas de AWS KMS API em um. Conta da AWS A menos que a política de chaves permita isto explicitamente, você não

pode usar políticas do IAM para autorizar o acesso a uma chave do KMS. Sem permissão da política de chaves, as políticas do IAM que autorizam permissões não têm efeito. Para obter mais informações, consulte Permitir que as políticas do IAM permitam o acesso à chave do KMS.

- É possível usar uma política do IAM para negar o acesso a uma chave gerenciada pelo cliente sem a permissão correspondente da política de chaves.
- Ao projetar políticas de chaves e políticas do IAM para chaves de várias regiões, considere o seguinte:
  - Políticas de chaves não são propriedades compartilhadas de chaves de várias regiões e não são copiadas nem sincronizadas entre chaves de várias regiões relacionadas.
  - Quando uma chave de várias regiões é criada usando as ações `CreateKey` e `ReplicateKey`, a política de chave padrão é aplicada a menos que uma política de chave seja especificada na solicitação.
  - Você pode implementar chaves de condição, como aws: RequestedRegion, para limitar as permissões a uma determinada Região da AWS.
  - É possível usar concessões para dar permissões para uma chave primária ou chave de réplica de várias regiões. Porém, não é possível usar uma única concessão para dar permissões para várias chaves do KMS, mesmo que elas sejam chaves de várias regiões relacionadas.

Ao usar AWS KMS e criar políticas de chaves, considere as seguintes práticas recomendadas de criptografia e outras práticas recomendadas de segurança:

- Siga as recomendações dos seguintes recursos para obter as AWS KMS melhores práticas:
  - Melhores práticas para AWS KMS subsídios (AWS KMS documentação)
  - Práticas recomendadas para políticas do IAM (documentação do AWS KMS)
- De acordo com a prática recomendada de separação de funções, mantenha identidades separadas para aqueles que administram as chaves e aqueles que as usam:
  - Os perfis de administrador que criam e excluem chaves não devem ter a capacidade de usar a chave.
  - Alguns serviços podem precisar apenas criptografar dados e não devem ter a capacidade de descriptografar os dados usando a chave.
- As políticas de chaves devem sempre seguir um modelo de privilégio mínimo. Não use o `kms:*` para ações no IAM ou nas políticas de chaves, pois isso concede às entidades principais permissões para administrar e usar a chave.

- Limite o uso de chaves gerenciadas Serviços da AWS pelo cliente a específicas usando a chave de ViaService condição kms: dentro da política de chaves.
- Se for necessário escolher entre tipos de chave, as chaves gerenciadas pelo cliente devem ser preferidas porque oferecem as opções de controle mais granulares, incluindo:
  - Gerenciar a autenticação e o controle de acesso
  - Habilitar e desabilitar chaves
  - Alternar AWS KMS keys
  - Marcar chaves com tags
  - Criar aliases
  - Excluir AWS KMS keys
- AWS KMS as permissões administrativas e de modificação devem ser explicitamente negadas a diretores não aprovados e as permissões de AWS KMS modificação não devem existir em uma declaração de permissão para diretores não autorizados. Para obter mais informações, consulte Ações, recursos e chaves de condição do AWS Key Management Service.
- Para detectar o uso não autorizado de chaves KMS, implemente as regras AWS Config-kms-actions e iam-customer-policy-blocked-kms-actions. iam-inline-policy-blocked Isso impede que os diretores usem as ações de AWS KMS descriptografia em todos os recursos.
- Implemente políticas de controle de serviço (SCPs) AWS Organizations para evitar que usuários ou funções não autorizados excluam as chaves do KMS, diretamente como um comando ou por meio do console. Para obter mais informações, consulte Usando SCPs como controles preventivos (AWS postagem no blog).
- Registre as chamadas da AWS KMS API no CloudTrail registro. Isso registra os atributos do evento relevante, como quais solicitações foram feitas, o endereço IP de origem do qual a solicitação foi feita e quem a fez. Para obter mais informações, consulte Logging AWS KMS API call with AWS CloudTrail.
- Se você usa contexto de criptografia, ele não deve conter nenhuma informação confidencial. CloudTrail armazena o contexto de criptografia em arquivos JSON de texto simples, que podem ser visualizados por qualquer pessoa com acesso ao bucket do S3 que contém as informações.
- Ao monitorar o uso de chaves gerenciadas pelo cliente, configure eventos para notificá-lo se ações específicas forem detectadas, como criação de chaves, atualizações em políticas de chaves gerenciadas pelo cliente ou importação de material de chaves. Também é recomendável implementar respostas automatizadas, como uma função do AWS Lambda que desabilita a chave ou executa qualquer outra ação de resposta a incidentes, conforme ditado pelas políticas organizacionais.

- Chaves de várias regiões são recomendadas para cenários específicos, como conformidade, recuperação de desastres ou backups. As propriedades de segurança das chaves de várias regiões são significativamente diferentes das chaves de uma única região. As seguintes recomendações se aplicam ao autorizar a criação, o gerenciamento e o uso de chaves de várias regiões:
  - Permita que as entidades principais repliquem uma chave de várias regiões apenas nas Regiões da AWS que precisam dessa chave.
  - Dê permissão para chaves de várias regiões apenas às entidades principais que precisam delas e apenas para tarefas necessárias.

AWS Lambda

O AWS Lambda é um serviço de computação que ajuda a executar código sem exigir provisionamento ou gerenciamento de servidores. Para proteger suas variáveis de ambiente, você pode usar a criptografia do lado do servidor para proteger seus dados em repouso e a criptografia do lado do cliente para proteger seus dados em trânsito.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- O Lambda sempre fornece criptografia do lado do servidor em repouso com AWS KMS key. Por padrão, o Lambda usa uma chave AWS gerenciada. Recomendamos usar uma chave gerenciada pelo cliente porque você tem controle total sobre a chave, incluindo gerenciamento, alternância e auditoria.
- Para dados em trânsito que exigem criptografia, ative os auxiliares, o que garante que as variáveis do ambiente sejam criptografadas no lado do cliente para a proteção em trânsito com a chave do KMS de sua preferência. Para obter mais informações, consulte Segurança em trânsito em Proteger variáveis do ambiente.
- As variáveis de ambiente da função do Lambda que contêm dados confidenciais ou críticos devem ser criptografadas em trânsito para ajudar a proteger os dados que são transmitidos dinamicamente para as funções (geralmente informações de acesso) contra acesso não autorizado.
- Para impedir que um usuário visualize variáveis de ambiente, adicione uma declaração às permissões do usuário na política do IAM ou na política de chave que negue o acesso à chave padrão, a uma chave gerenciada pelo cliente ou a todas as chaves. Para obter mais informações, consulte Usar variáveis de ambiente do AWS Lambda.

Amazon Relational Database Service

O Amazon Relational Database Service (Amazon RDS) ajuda você a configurar, operar e escalar um banco de dados (DB) relacional na Nuvem AWS. Os dados criptografados em repouso incluem o armazenamento subjacente para instâncias de banco de dados, seus backups automatizados, réplicas de leitura e snapshots.

As abordagens que podem ser usadas para criptografar dados em repouso em instâncias de banco de dados do RDS são:

- Você pode criptografar instâncias de banco de dados do Amazon RDS com AWS KMS keys uma chave AWS gerenciada ou uma chave gerenciada pelo cliente. Para obter mais informações, consulte AWS Key Management Service neste guia.
- O Amazon RDS para Oracle e o Amazon RDS para SQL Server oferecem suporte à criptografia de instâncias de banco de dados com o Transparent Data Encryption (TDE). Para obter mais informações, consulte Oracle Transparent Data Encryption ou Suporte ao Transparent Data Encryption no SQL Server.

É possível usar chaves do TDE e do KMS para criptografar instâncias de banco de dados. No entanto, isso pode afetar um pouco a performance do banco de dados. Por isso, essas chaves devem ser gerenciadas separadamente.

As abordagens que podem ser usadas para criptografar dados em trânsito de ou para instâncias de banco de dados do RDS são:

- Para uma instância de banco de dados do Amazon RDS com MariaDB, Microsoft SQL Server, MySQL, Oracle ou PostgreSQL, é possível usar SSL para criptografar a conexão. Para obter mais informações, consulte Usar SSL/TLS para criptografar uma conexão para uma instância de banco de dados.
- O Amazon RDS para Oracle também oferece suporte à criptografia de rede nativa (NNE) da Oracle, a qual criptografa os dados enquanto ele é transferido de/para uma instância de banco de dados. Não é possível usar criptografia NNE e SSL ao mesmo tempo. Para ter mais informações, consulte Oracle Native Network Encryption.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Ao se conectar a instâncias de banco de dados Amazon RDS para SQL Server ou Amazon RDS para PostgreSQL para processar, armazenar ou transmitir dados que exijam criptografia, use o recurso RDS Transport Encryption para criptografar a conexão. Para isso, defina o parâmetro `rds.force_ssl` como 1 no grupo de parâmetros. Para obter mais informações, consulte Trabalhar com grupos de parâmetros. O Amazon RDS para Oracle usa criptografia de rede nativa do banco de dados Oracle.
- As chaves gerenciadas pelo cliente para criptografia de instâncias de banco de dados do RDS devem ser usadas somente para essa finalidade, e não com outros Serviços da AWS.
- Antes de criptografar uma instância de banco de dados do RDS, estabeleça os requisitos da chave do KMS. A chave usada pela instância não poderá ser alterada posteriormente. Por exemplo, em sua política de criptografia, defina padrões de uso e gerenciamento para chaves AWS gerenciadas ou chaves gerenciadas pelo cliente, com base nos requisitos da sua empresa.
- É altamente recomendável habilitar backups para instâncias de banco de dados do RDS criptografadas. O Amazon RDS pode perder o acesso à chave do KMS para uma instância de banco de dados, como quando a chave do KMS não está habilitada ou quando o acesso do RDS a uma chave do KMS é revogado. Se isso ocorrer, a instância de banco de dados criptografada entrará em um estado recuperável por sete dias. Se a instância de banco de dados não recuperar o acesso à chave após sete dias, o banco de dados se tornará totalmente inacessível e deverá ser restaurado a partir de um backup. Para obter mais informações, consulte Criptografar uma instância de banco de dados.
- Se uma réplica de leitura e sua instância de banco de dados criptografada estiverem na mesma Região da AWS, você deverá usar a mesma chave KMS para criptografar ambas.
- Em AWS Config, implemente a regra rds-storage-encrypted AWS gerenciada para validar e aplicar a criptografia para instâncias de banco de dados do RDS e a rds-snapshots-encryptedregra para validar e aplicar a criptografia para instantâneos do banco de dados do RDS.

AWS Secrets Manager

O AWS Secrets Manager ajuda a substituir credenciais codificadas, incluindo senhas, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação. O Secrets Manager se AWS KMS integra para criptografar cada versão de cada valor secreto com uma chave de dados exclusiva que é protegida por um. AWS KMS key Essa integração protege segredos armazenados com chaves de criptografia que nunca saem AWS KMS sem criptografia. Também é possível definir permissões personalizadas na chave do KMS para auditar as operações que geram, criptografam e descriptografam as chaves de dados que protegem seus segredos armazenados.

Para obter mais informações, consulte Criptografia e descriptografia de dados no AWS Secrets Manager.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Na política de chaves, use a chave de ViaService condição kms: para limitar o uso da chave somente a solicitações do Secrets Manager atribuindo o valor. `secretsmanager.<region>.amazonaws.com`
- Para obter segurança adicional, com base nos requisitos de negócios, use chaves ou valores n ocontexto de criptografia do Secrets Manager como condição para usar a chave do KMS criando:
  - Um operador de condição de string em uma política do IAM ou de chave
  - Uma restrição de concessão em uma concessão
- Em AWS Config, implemente a regra secretsmanager-using-cmk AWS gerenciada para verificar se todos os segredos no Secrets Manager estão criptografados com uma chave KMS AWS gerenciada ou uma chave KMS gerenciada pelo cliente.
- Para garantir que os segredos estejam em conformidade com as políticas de rotação definidas, implemente as seguintes AWS Config regras:
  - secretsmanager-rotation-enabled-check— Verifica se a rotação está configurada para segredos armazenados no Secrets Manager.
  - secretsmanager-scheduled-rotation-success-check — Verifica se os segredos foram rotacionados com sucesso. AWS Config também verifica se a última data de rotação está dentro da frequência de rotação configurada.
  - secretsmanager-secret-periodic-rotation— Verifica se os segredos foram alternados dentro do número de dias especificado.
  - secretsmanager-secret-unused— Verifica se os segredos foram acessados dentro do número de dias especificado.
- Use AWS CloudTrail para registrar todas as chamadas de API para o Secrets Manager e eventos não relacionados à API, como início da rotação, sucesso da rotação, falhas de rotação e exclusão programada de segredos. Para obter mais informações, consulte Registrar AWS Secrets Manager eventos com AWS CloudTrail.
- Use o Amazon CloudWatch Events para configurar alertas para algumas operações do Secrets Manager, como excluir segredos, alternar segredos ou tentar usar um segredo programado para exclusão. É possível escolher quais operações acionam um alerta. O alerta pode ser um tópico do SNS que envia um e-mail ou uma mensagem de texto para os assinantes ou uma função do Lambda que registra os detalhes da operação para análise posterior.

Amazon Simple Storage Service

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos baseado na nuvem que ajuda você a armazenar, proteger e recuperar qualquer quantidade de dados.

Para a criptografia do lado do servidor no Amazon S3, há três opções:

- Criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3)
- Criptografia do lado do servidor com AWS Key Management Service (SSE-KMS)
- Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Se a criptografia do lado do servidor for usada para criptografar um objeto no momento do upload, adicione o cabeçalho `x-amz-server-side-encryption` à solicitação para que o Amazon S3 criptografe o objeto usando SSE-S3, SSE-KMS ou SSE-C. Os possíveis valores para o cabeçalho `x-amz-server-side-encryption` são:

- `AES256`, que instrui o Amazon S3 a usar chaves gerenciadas pelo Amazon S3.
- `aws:kms`, que instrui o Amazon S3 a usar chaves AWS KMS gerenciadas.
- Definir o valor como `True` ou `False` para SSE-C

Para obter mais informações, consulte o efense-in-depth requisito D 1: Os dados devem ser criptografados em repouso e durante o trânsito em Como usar políticas de bucket e aplicar defesa profunda para ajudar a proteger seus dados do Amazon S3 (postagem no blog).AWS

Para a criptografia do lado do servidor no Amazon S3, há duas opções:

- Uma chave armazenada em AWS KMS
- Uma chave armazenada na aplicação

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Em AWS Config, implemente a regra bucket-server-side-encryption AWS gerenciada habilitada para s3 para validar e aplicar a criptografia do bucket S3.
- Implante uma política de bucket do Amazon S3 que valide que todos os objetos que estão sendo carregados sejam criptografados usando a condição `s3:x-amz-server-side-encryption`.

Para obter mais informações, consulte o exemplo de política de bucket em Proteger dados usando SSE-S3 e as instruções em Adicionar uma política de bucket.

- Permita que somente conexões criptografadas por HTTPS (TLS) usando a condição `aws:SecureTransport` nas políticas de bucket do S3. Para obter mais informações, consulte Qual política de bucket do S3 devo usar para cumprir a AWS Config regra s3-? bucket-ssl-requests-only
- Em AWS Config, implemente a regra bucket-ssl-requests-only AWS gerenciada por s3 para exigir que as solicitações usem SSL.
- Use uma chave gerenciada pelo cliente quando for necessário conceder acesso entre contas a objetos do Amazon S3. Configure a política de chaves para permitir o acesso de outra Conta da AWS.

Amazon Virtual Private Cloud

A Amazon Virtual Private Cloud (Amazon VPC) ajuda você a lançar AWS recursos em uma rede virtual que você definiu. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS.

Considere as seguintes práticas recomendadas de criptografia para esse serviço:

- Criptografe o tráfego entre ativos de informação e sistemas dentro da rede corporativa VPCs usando uma das seguintes opções:
  - AWS Site-to-Site VPN conexões
  - Uma combinação de AWS Direct Connect conexões AWS Site-to-Site VPN e, que fornece uma conexão privada criptografada por IPsec
  - AWS Direct Connect conexões que oferecem suporte ao MAC Security (MACsec) para criptografar dados de redes corporativas até o local AWS Direct Connect
- Use VPC endpoints para conectar de forma privada suas VPCs AWS PrivateLink às VPCs suportadas Serviços da AWS sem usar um gateway de internet. Você pode usar AWS Direct Connect nossos AWS VPN serviços para estabelecer essa conexão. O tráfego entre sua VPC e o outro serviço não sai da AWS rede. Para obter mais informações, consulte Acesso Serviços da AWS por meio de AWS PrivateLink.
- Configure regras de grupo de segurança que permitam tráfego somente de portas associadas a protocolos seguros, como HTTPS sobre TCP/443. Audite periodicamente os grupos de segurança e suas regras.

Recursos

- Criar uma estratégia de criptografia corporativa para dados em repouso
- Práticas recomendadas de segurança para o AWS Key Management Service
- Como os Serviços da AWS usam o AWS KMS

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

função agregada

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

AI

Veja inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicativos

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter mais informações sobre como as AIOps são usadas na estratégia de migração para a AWS , 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.

Availability Zone (zona de disponibilidade)

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

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

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

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

B

bot ruim

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

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

acesso em vidro quebrado

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

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

planejamento de continuidade de negócios (BCP)

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

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

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

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja a integração e a entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de Excelência da 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 postagens do CCoE 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 geralmente está conectada à tecnologia de computação de ponta.

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

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

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

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

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

Um campo da IA que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, AWS Panorama oferece dispositivos que adicionam CV às redes de câmeras locais, e a Amazon SageMaker fornece algoritmos de processamento de imagem para CV.

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

desvio de dados

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

dados em trânsito

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

malha de dados

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

implantação

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

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Consulte linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja a recuperação de desastres.

detecção de deriva

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

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

computação de borda

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

Criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja o endpoint do serviço.

serviço de endpoint

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

planejamento de recursos corporativos (ERP)

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

criptografia envelopada

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

environment (ambiente)

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

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.

- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um pipeline de CI/CD, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

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

ERP

Consulte planejamento de recursos corporativos.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

falham rapidamente

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

limite de isolamento de falhas

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

ramificação de recursos

Veja a filial.

recursos

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

importância do recurso

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

transformação de recursos

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

FGAC

Veja o controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

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

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

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

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet das Coisas Industrial (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 Construir uma estratégia de transformação digital para a Internet das Coisas Industrial (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 segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação 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 machine learning com a AWS.

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

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

ramificação principal

Veja a filial.

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações confidenciais ou obter acesso

não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

conta-membro

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

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

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

microsserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. 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 APIs leves. 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 o. Nuvem AWS O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A ferramenta MPA (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja o aprendizado de máquina.

modernização

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

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um

esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliação da prontidão para modernização de aplicativos no. Nuvem AWS

aplicações monolíticas (monólitos)

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

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

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

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

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

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

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

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (OT)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

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

OU

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação 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

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pressão de predicados

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

controle preventivo

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

principal (entidade principal)

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

Privacidade por design

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

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas ao DNS para um domínio e seus subdomínios dentro de uma ou mais VPCs. Para obter mais informações, consulte Como trabalhar com zonas hospedadas privadas na documentação do Route 53.

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

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

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.

publicar/assinar (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

ransomware

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

Matriz RASCI

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

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

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

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

rotação

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

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

S

SAML 2.0

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto

e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte O que há em um segredo do Secrets Manager? na documentação do Secrets Manager.

controle de segurança

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

fortalecimento da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. As SCPs definem barreiras de proteção ou estabelecem limites para as ações que um administrador pode delegar a usuários ou perfis. É possível usar SCPs como listas de permissão ou de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte Políticas de controle de serviço na AWS Organizations documentação.

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

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

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

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

CUSPE

Veja um único ponto de falha.

esquema de estrelas

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

padrão strangler fig

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

sub-rede

Um intervalo de endereços IP na VPC. Uma sub-rede deve residir em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja o ambiente.

treinamento

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

gateway de trânsito

Um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte O que é um gateway de trânsito na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja o ambiente.

V

aspiração

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

controle de versões

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

emparelhamento de VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte o AWS Workload Qualification Framework.

escreva uma vez, leia muitas (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

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.