AWS Arquitetura de referência de privacidade

AWS Orientação prescritiva

AWS Orientação prescritiva: AWS Arquitetura de referência de privacidade

Table of Contents

AWS Arquitetura de referência de privacidade

Amazon Web Services (colaboradores)

Setembro de 2025 (histórico do documento)

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Notices

Este guia é fornecido apenas para fins informativos. Não é aconselhamento jurídico e não deve ser considerado como aconselhamento jurídico. AWS incentiva seus clientes a obter aconselhamento adequado sobre a implementação de ambientes de privacidade e proteção de dados e, de forma mais geral, de leis aplicáveis relevantes aos seus negócios.

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa as ofertas e práticas atuais de AWS produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de suas afiliadas, AWS fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas.

As responsabilidades e obrigações de AWS seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum contrato entre AWS e seus clientes.

Introdução

A Arquitetura AWS de Referência de Privacidade (AWS PRA) fornece um conjunto de diretrizes específicas para o design e a configuração de controles de suporte à privacidade em. Serviços da AWS Este guia pode ajudar você a tomar decisões sobre pessoas, processos e tecnologias que ajudam a apoiar a privacidade na Nuvem AWS.

O modelo de responsabilidade AWS compartilhada e a privacidade

No Nuvem AWS, você compartilha a responsabilidade pela segurança e conformidade com AWS. AWS é responsável pela segurança da nuvem, o que significa que AWS é responsável por proteger a infraestrutura que executa todos os serviços oferecidos no Nuvem AWS. Você é responsável pela segurança na nuvem, o que significa que você é responsável por configurar e gerenciar Serviços da AWS de acordo com os requisitos de segurança e privacidade. Para obter mais informações, consulte o modelo de responsabilidade compartilhada da AWS.

Serviços da AWS fornecem recursos que permitem que você implemente seus próprios controles de privacidade na nuvem para atender aos seus requisitos de privacidade. Sua responsabilidade de privacidade varia com base em muitos fatores, incluindo o Serviços da AWS Regiões da AWS que você escolhe, a integração desses serviços em seu ambiente de TI e as leis e regulamentos aplicáveis à sua organização e carga de trabalho.

Ao usar Serviços da AWS, você mantém o controle sobre seu conteúdo. Especificamente, o conteúdo do cliente é definido como software (incluindo imagens de máquinas), dados, texto, áudio, vídeo ou imagens que você ou qualquer usuário final transfere para nós para processamento, armazenamento ou hospedagem Serviços da AWS em conexão com sua conta. Também inclui todos os resultados computacionais que você ou um usuário final obtêm usando. Serviços da AWS Você é responsável por gerenciar as seguintes decisões, que estão sob seu controle:

- Os dados que você escolhe coletar, armazenar ou processar AWS
- O Serviços da AWS que você usa com os dados
- Região da AWS Onde você coleta, armazena ou processa dados
- O formato e a estrutura dos seus dados e se eles estão mascarados, anônimos ou criptografados
- Como você define, armazena, gira e opera suas chaves criptográficas para criptografia
- Quem tem acesso e quando tem acesso aos seus dados e como esses direitos de acesso são concedidos, gerenciados e revogados

Depois de entender o modelo de responsabilidade AWS compartilhada e como ele geralmente se aplica à operação na nuvem, você deve determinar como ele se aplica ao seu caso de uso. O Serviços da AWS que você escolhe usar determina a quantidade de configuração que você deve executar como parte das responsabilidades de privacidade da sua organização. Por exemplo, um serviço como o Amazon Elastic Compute Cloud (Amazon EC2) é categorizado como infraestrutura como serviço (IaaS). Dessa forma, se você usa o Amazon EC2, deve realizar todas as configurações

de privacidade necessárias para sistemas operacionais convidados e para o software ou utilitários da aplicação que você instala em suas instâncias do EC2. Quando você usa um serviço abstrato, como o Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB AWS , é responsável pela camada de infraestrutura, pelo sistema operacional e pelas plataformas. Sua responsabilidade é gerenciar e classificar os dados (conteúdo do cliente) e configurar as políticas usadas para acessar os endpoints a fim de armazenar e recuperar dados. Para obter mais informações sobre como AWS ajudar você a proteger dados e privacidade, consulte Proteção de dados e privacidade em AWS.

Entendendo o AWS PRA

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

A seção descreve a relação entre a Arquitetura AWS de Referência de Privacidade (AWS PRA) e outras AWS diretrizes. Esta seção também analisa o layout geral e a estrutura do exemplo de ambiente de AWS várias contas no AWS PRA.

Esta seção contém os seguintes tópicos:

- Usando o AWS PRA e o AWS SRA
- AWS Organizations e a estrutura de conta dedicada
- Operacionalizando AWS serviços de privacidade

Usando o AWS PRA e o AWS SRA

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

O AWS PRA fornece padrões que os clientes consideraram úteis no planejamento de controles de privacidade básicos e em nível de aplicativo para sua infraestrutura e cargas de trabalho em. AWS A AWS Security Reference Architecture (AWS SRA) fornece um conjunto de diretrizes para criar uma arquitetura que implemente e ofereça suporte ao conjunto certo de controles de segurança em sua AWS landing zone e seus aplicativos. Para estabelecer os controles de privacidade detalhados neste guia, o AWS PRA assume muitas das mesmas diretrizes fundamentais e estrutura de conta descritas no AWS SRA. O AWS PRA e o AWS SRA detalham muitas das mesmas chaves Serviços da AWS. Este guia inclui apenas breves descrições desses serviços. Você pode aprender mais sobre esses serviços e como eles são usados em um contexto de segurança no AWS SRA.

O AWS SRA pode ajudá-lo a projetar, implementar e gerenciar serviços de AWS segurança para que eles se alinhem às práticas AWS recomendadas. Você pode usar o AWS SRA como um guia independente ou pode usar o AWS SRA e o AWS PRA como guias complementares. Muitas das diretrizes de segurança detalhadas no AWS SRA podem ser seguidas em conjunto com os controles de privacidade detalhados no PRA. AWS Semelhante à segurança, há considerações fundamentais sobre privacidade que podem ser úteis no início de sua jornada para a Nuvem AWS , pois essas decisões podem afetar o design da estrutura de contas da organização. Por exemplo, algumas perguntas que você pode considerar incluem:

- Como minha organização define dados pessoais?
- Minha organização oferece suporte a aplicações que processam dados pessoais?
- E quanto às aplicações que processam outros tipos de dados regulamentados?
- Quais controles em nível organizacional posso implementar para manter meus desenvolvedores e engenheiros de nuvem o mais longe possível dos dados pessoais?
- Como faço para segmentar dados pessoais de outros tipos de dados?
- Quais são os requisitos de transferência de dados transfronteiriça da minha organização?

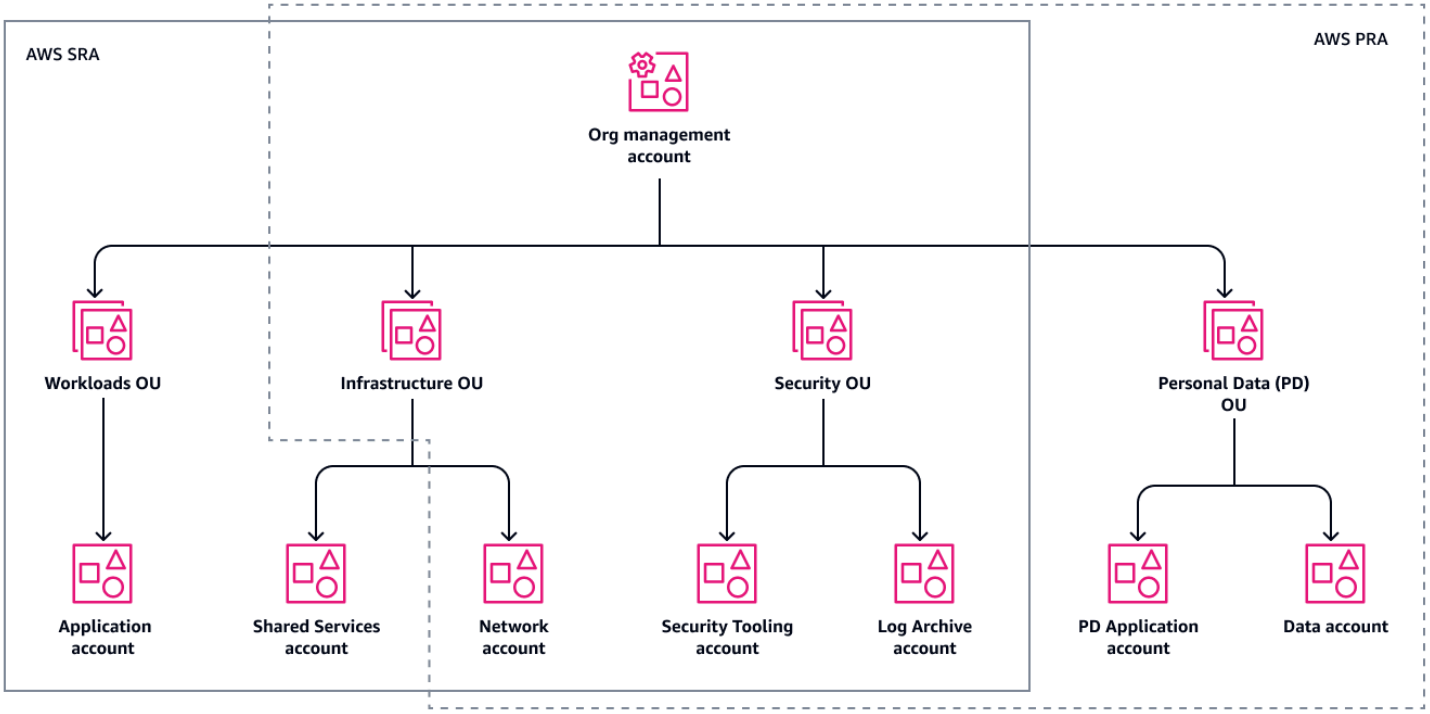
As respostas para muitas dessas perguntas podem ter implicações no design do seu ambiente de nuvem, como sua Conta da AWS estrutura, políticas de controle de serviços e funções AWS Identity and Access Management (IAM).

AWS Organizations e a estrutura de conta dedicada

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

O AWS Organizations é um serviço de gerenciamento de contas que ajuda a gerenciar e governar de forma centralizada várias Contas da AWS. O uso do AWS Organizations é a base de um ambiente bem arquitetado e com várias AWS contas. Para obter mais informações, consulte Establishing your best practice AWS environment.

O diagrama a seguir mostra a estrutura de contas e unidades organizacionais (OU) de alto nível do AWS PRA. Na maioria das vezes, a estrutura organizacional do AWS PRA corresponde à estrutura organizacional do AWS SRA.



Os desvios da organização da AWS SRA incluem:

- O AWS PRA adiciona a OU de Dados Pessoais (PD), que é dedicada à coleta, armazenamento e processamento de dados pessoais. Essa separação estrutural fornece flexibilidade para que você possa definir controles específicos e refinados para ajudar a proteger os dados pessoais da divulgação não intencional.
- Na UO de Infraestrutura, o AWS PRA atualmente não inclui orientações adicionais para a conta de Serviços Compartilhados descrita na AWS SRA.
- Atualmente, o AWS PRA não inclui orientações adicionais para a OU de cargas de trabalho descritas na AWS SRA. As aplicações que coletam ou processam dados pessoais estão localizadas em contas dedicadas na UO de dados pessoais.

Você pode usar o AWS Control Tower para governança básica geral e implantação automatizada de controles de segurança e privacidade em toda a sua organização. Se AWS Control Tower não estiver em uso atualmente em sua organização, você ainda pode implantar muitos dos controles de segurança e privacidade AWS Control Tower, como políticas e AWS Config regras de controle de serviços, em seus respectivos serviços.

Talvez seja útil considerar o processamento de dados pessoais ao planejar sua conta e a estrutura da UO, incluindo uma estratégia de segmentação de contas. Talvez seja necessário considerar os tipos de dados que você está processando para seus casos de uso exclusivos e as leis e regulamentações aplicáveis. Por exemplo, os dados do titular do cartão são protegidos pelo Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS), e as informações de saúde protegidas podem estar sujeitas à Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA). Talvez você queira analisar quais ambientes contêm dados pessoais e planejar sua estratégia de segmentação com base nisso. Uma estratégia típica de segmentação de contas pode incluir Contas da AWS dedicadas que se alinham ao ciclo de vida de desenvolvimento de software (SDLC), como contas dedicadas para desenvolvimento, preparação ou garantia de qualidade (QA) e produção. Uma estratégia de segmentação como essa pode ser um componente essencial na discussão geral do projeto, e OUs talvez seja necessário se alinhar aos requisitos regulatórios específicos.

Alguns AWS ambientes com várias contas exigem contas de aplicativos dedicadas por Região da AWS, ou podem exigir zonas de destino com várias contas. Nesse caso, você precisa de segmentação adicional para atender aos requisitos exclusivos de soberania de dados de seus clientes e reguladores. Para obter mais informações, consulte Elaboração de estratégias para uma expansão global neste guia.

Operacionalizando AWS serviços de privacidade

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Para muitos, a privacidade é transversal. Muitas equipes diferentes têm um papel a desempenhar, incluindo equipes regulatórias, de conformidade e de engenharia. Quando sua organização começar a definir as principais pessoas e os componentes de políticas do seu programa de privacidade, você poderá mapear os controles em relação a um framework de conformidade de privacidade para operações consistentes. Uma estrutura pode servir como uma rubrica para implementar controles de privacidade básicos e específicos do aplicativo para dados pessoais em seu ambiente. AWS

Independentemente do framework que os clientes usam para categorizar seus requisitos de privacidade, as equipes de conformidade de privacidade, engenharia de privacidade e aplicações

geralmente precisam trabalhar juntas para atingir as metas de implementação. Por exemplo, as equipes regulatórias e de conformidade podem fornecer os requisitos de alto nível, e as equipes de engenharia e aplicativos configuram Serviços da AWS e apresentam recursos para se alinharem a esses requisitos. Começar com um framework de controle pode ajudar a definir controles organizacionais e técnicos mais prescritivos.

Ao definir os controles técnicos Serviços da AWS e os recursos, outra decisão importante é se um controle deve ser aplicado a toda a organização, a uma OU, a uma conta ou a um recurso específico. Alguns serviços e recursos são ideais para implementar controles em toda a AWS organização. Por exemplo, bloquear o acesso público aos buckets do Amazon S3 é um controle específico que é configurado preferencialmente na raiz da organização, em vez de individualmente para cada conta. No entanto, suas políticas de retenção podem variar de aplicação para aplicação, o que significa que você pode aplicar o controle no nível do recurso.

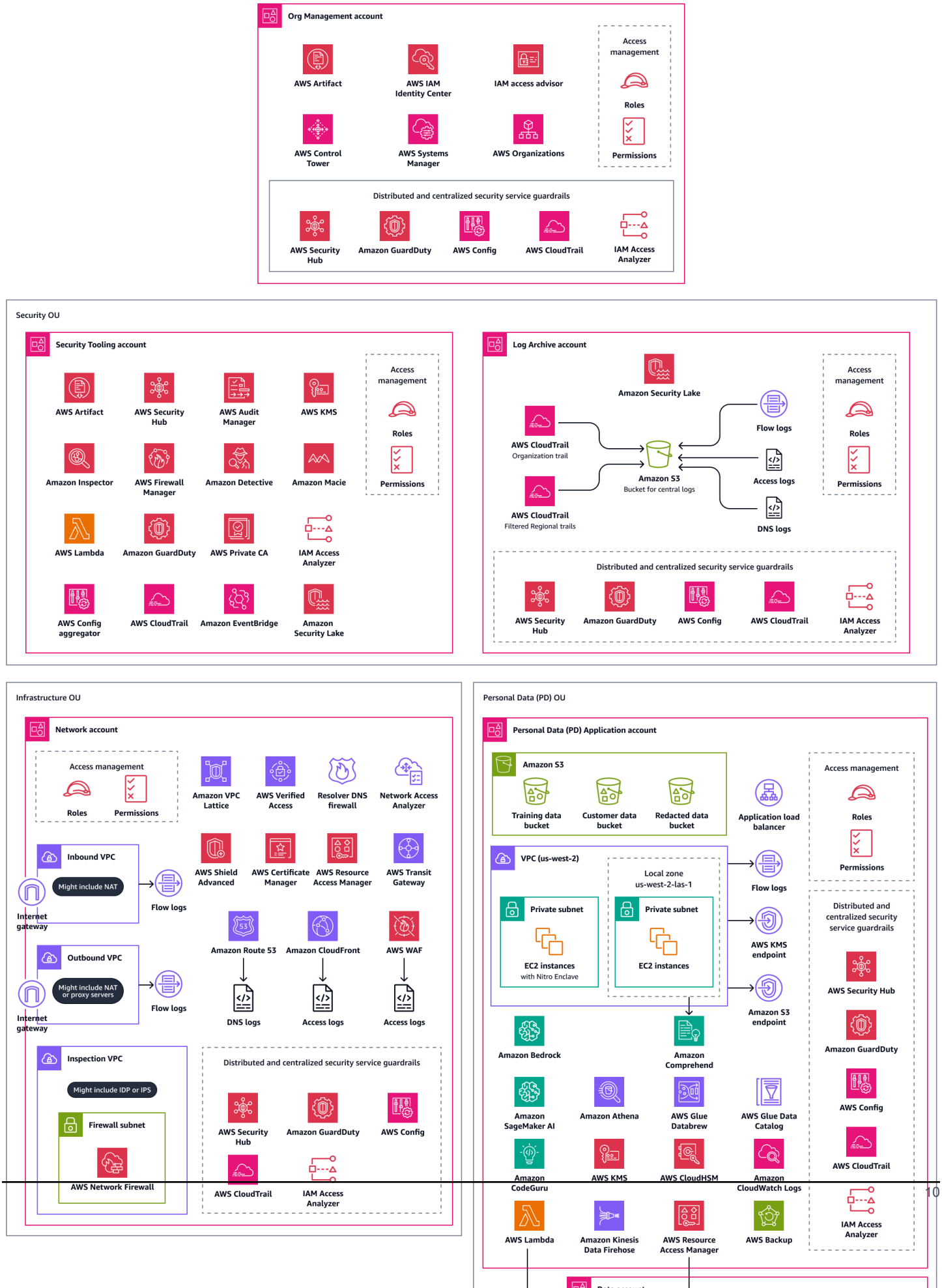
Para ajudá-lo a acelerar a operacionalização da privacidade em sua organização, AWS oferece serviços de consultoria de auditoria e conformidade para suas AWS cargas de trabalho. Para obter mais informações, entre em contato com o AWS SAS.

A arquitetura AWS de referência de privacidade

Pesquisa

Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

O diagrama a seguir ilustra a Arquitetura AWS de Referência de Privacidade (AWS PRA). Esse é um exemplo de uma arquitetura que conecta muitos recursos e recursos relacionados à privacidade Serviços da AWS . Essa arquitetura é criada em uma zona de pouso que é governada pelo AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Amazon Security Lake
Log Archive account
Amazon Security Lake
AWS CloudTrail
Organization trail
Flow logs
Access logs
Amazon S3
Bucket for central logs
AWS CloudTrail
Filtered Regional trails
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

O AWS PRA inclui uma arquitetura web sem servidor que é hospedada na conta do aplicativo de dados pessoais (PD). A arquitetura dessa conta é um exemplo de workload que coleta dados pessoais diretamente dos consumidores. Nessa workload, os usuários se conectam por meio de uma camada da web. A camada da web interage com a camada da aplicação. Essa camada recebe informações da camada da web, processa e armazena os dados, permite que equipes internas autorizadas e terceiros acessem os dados e, por fim, arquiva e exclui os dados quando não são mais necessários. A arquitetura é propositadamente modular e orientada por eventos para demonstrar muitas das técnicas básicas de engenharia de privacidade sem se aprofundar em casos de uso específicos, como data lakes, contêineres, computação ou Internet das Coisas (IoT).

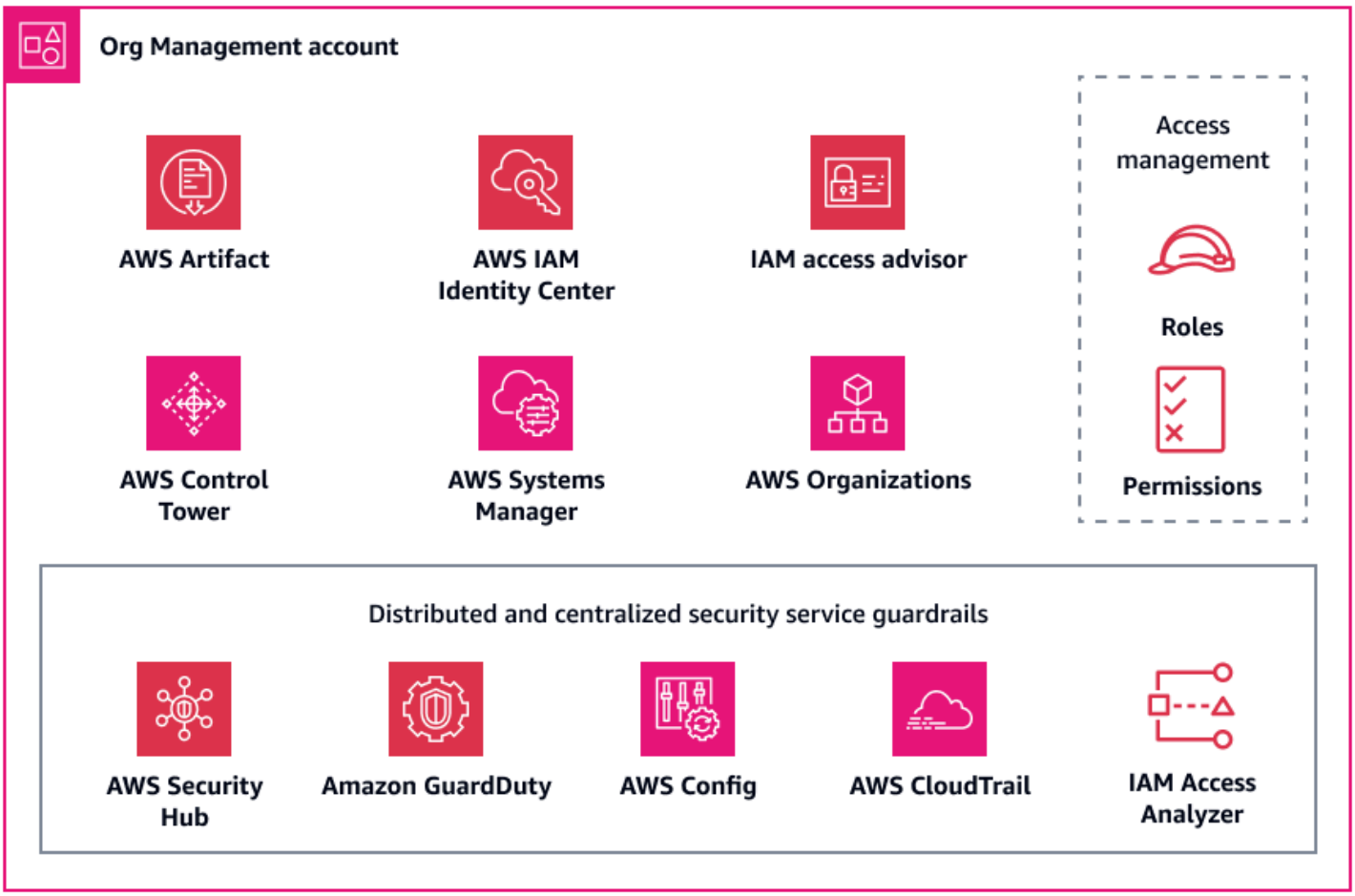
A seguir, este guia descreve detalhadamente cada conta na organização. Ele discute os serviços e recursos relacionados à privacidade, as considerações e recomendações e os diagramas de cada uma das seguintes contas:

- Conta gerencial da organização
- UO de segurança | Conta do Security Tooling
- UO de segurança | Conta do Log Archive
- Infraestrutura de UO: conta de Rede
- UO de dados pessoais | Conta do PD Application

Conta gerencial da organização

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

A conta gerencial da organização é usada principalmente para gerenciar a variação da configuração de recursos dos controles básicos de privacidade em todas as contas da sua organização, que é gerenciada pelo AWS Organizations. Essa conta também é onde você pode implantar novas contas de membros de forma consistente, com muitos dos mesmos controles de segurança e privacidade. Para obter mais informações sobre essa conta, consulte a Arquitetura AWS de Referência de Segurança (AWS SRA). O diagrama a seguir ilustra os serviços de AWS segurança e privacidade configurados na conta de gerenciamento da organização.



Esta seção fornece informações mais detalhadas sobre os seguintes Serviços da AWS que são usados nessa conta:

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

O AWS Artifact pode ajudar você com auditorias fornecendo downloads sob demanda de documentos e segurança e conformidade da AWS . Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Isso AWS service (Serviço da AWS) ajuda você a entender os controles que você herda AWS e a determinar quais controles podem estar faltando para você implementar em seu ambiente. AWS Artifact fornece acesso a relatórios AWS de segurança e conformidade, como relatórios de controles

do sistema e da organização (SOC) e relatórios do setor de cartões de pagamento (PCI). Ele também fornece acesso a certificações de órgãos de credenciamento em todas as regiões e setores de conformidade que validam a implementação e a eficácia operacional dos controles. AWS Usando AWS Artifact, você pode fornecer os artefatos de AWS auditoria aos seus auditores ou reguladores como evidência dos controles de AWS segurança e privacidade. Os relatórios a seguir podem ser úteis para demonstrar a eficácia dos controles de privacidade da AWS :

- Relatório de privacidade SOC 2 tipo 2 — Este relatório demonstra a eficácia dos AWS controles sobre como os dados pessoais são coletados, usados, retidos, divulgados e descartados. Há também um relatório SOC 3 Privacidade, que é uma descrição menos detalhada dos controles de privacidade do SOC 2. Para obter mais informações, consulte as Perguntas frequentes sobre o SOC.
- Catálogo de controles de conformidade de computação em nuvem (C5): este relatório foi criado pela autoridade nacional de segurança cibernética da Alemanha, Bundesamt für Sicherheit in der Informationstechnik (BSI). Ele detalha os controles de segurança que a AWS implementou para atender aos requisitos do C5. Também inclui requisitos adicionais de controle de privacidade relacionados à localização de dados, ao provisionamento de serviços, ao local de jurisdição e às obrigações de divulgação de informações.
- Relatório de certificação ISO/IEC 27701:2019: a ISO/IEC 27701:2019 descreve os requisitos e as diretrizes para estabelecer e melhorar continuamente um sistema de gerenciamento de informações de privacidade (PIMS). Esse relatório detalha o escopo dessa certificação e pode servir como prova de AWS certificação. Para obter mais informações sobre esse padrão, consulte ISO/IEC 27701:2019 (site da ISO).

AWS Control Tower

AWS Control Towerajuda você a configurar e controlar um ambiente de AWS várias contas que segue as práticas prescritivas recomendadas de segurança. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Em AWS Control Tower, você também pode automatizar a implantação de muitos controles proativos, preventivos e de deteção, também conhecidos como grades de proteção, que se alinham aos seus requisitos de privacidade de dados, especificamente para residência e soberania de dados. Por exemplo, você pode especificar barreiras de proteção que limitam a transferência de dados somente às Regiões da AWS aprovadas. Para um controle ainda mais granular, você pode escolher entre mais de 17 grades de proteção projetadas para controlar a residência dos dados, como Proibir

conexões Amazon Virtual Private Network (VPN), Proibir o acesso à Internet para uma instância do Amazon VPC e Negar acesso com base na solicitação. AWS Região da AWS Essas grades de proteção consistem em vários AWS CloudFormation ganchos, políticas de controle de serviços e AWS Config regras que podem ser implantadas uniformemente em sua organização. Para obter mais informações, consulte Controles que aprimoram a proteção da residência de dados na AWS Control Tower documentação.

Para soberania de dados, AWS Control Tower atualmente fornece controles preventivos, como Exigir que um volume anexado do Amazon EBS esteja configurado para criptografar dados em repouso e Exigir que uma política AWS KMS chave tenha uma declaração que limite a criação de concessões a. AWS KMS Serviços da AWS Os controles de soberania são mais amplos do que apenas controles de residência de dados. Eles ajudam a evitar ações que possam violar a residência de dados, a restrição granular de acesso, a criptografia e os requisitos de resiliência. Para obter mais informações, consulte Preventive controls that assist with digital sovereignty na documentação do AWS Control Tower .

Se você precisar implantar barreiras de privacidade além dos controles de residência e soberania de dados, AWS Control Tower inclua vários controles obrigatórios. Esses controles são implantados por padrão em todas as UO quando você configura a zona de pouso. Muitos deles são controles preventivos projetados para proteger os registros, como não permitir a exclusão do arquivo de registros e ativar a validação de integridade do arquivo de log. CloudTrail

AWS Control Tower também é integrado AWS Security Hub CSPM para fornecer controles de detetive. Esses controles são conhecidos como Service-Managed Standard:. AWS Control Tower Você pode usar esses controles para monitorar o desvio de configuração de controles de suporte à privacidade, como criptografia em repouso para as instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS).

AWS Organizations

O AWS PRA usa AWS Organizations para gerenciar centralmente todas as contas dentro da arquitetura. Para obter mais informações, consulte AWS Organizations e a estrutura de conta dedicada neste guia. Em AWS Organizations, você pode usar políticas de controle de serviços (SCPs) e políticas de gerenciamento para ajudar a proteger os dados pessoais e a privacidade.

Políticas de controle de serviços (SCPs)

As políticas de controle de serviço (SCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões em sua organização. Eles fornecem controle centralizado sobre o máximo

de permissões disponíveis para funções e usuários AWS Identity and Access Management (IAM) na conta de destino, na unidade organizacional (OU) ou na organização inteira. Você pode criar e se inscrever a SCPs partir da conta de gerenciamento da organização.

Você pode usar AWS Control Tower para implantar SCPs uniformemente em suas contas. Para obter mais informações sobre os controles de residência de dados pelos quais você pode se inscrever AWS Control Tower, consulte AWS Control Tower este guia. AWS Control Tower inclui um complemento completo de medidas preventivas SCPs. Se o AWS Control Tower não for usado atualmente em sua organização, você também pode implantar esses controles manualmente.

Usando SCPs para atender aos requisitos de residência de dados

É comum gerenciar os requisitos de residência de dados pessoais armazenando e processando dados em uma região geográfica específica. Para verificar se os requisitos exclusivos de residência de dados de uma jurisdição foram atendidos, recomendamos que você trabalhe em estreita colaboração com sua equipe regulatória para confirmar seus requisitos. Quando esses requisitos são determinados, há vários controles AWS básicos de privacidade que podem ajudar no suporte. Por exemplo, você pode usar SCPs para limitar o que Regiões da AWS pode ser usado para processar e armazenar dados. Para ver um exemplo de política, consulte Restrinja transferências de dados entre Regiões da AWS neste guia.

Usando SCPs para restringir chamadas de API de alto risco

É importante entender quais controles de segurança e privacidade são responsáveis e pelos quais você AWS é responsável. Por exemplo, você é responsável pelos resultados das chamadas de API que podem ser feitas em relação aos Serviços da AWS que você usa. Você também é responsável por entender quais dessas chamadas podem resultar em alterações em sua postura de segurança ou privacidade. Se você está preocupado em manter uma certa postura de segurança e privacidade, você pode habilitar SCPs essa negação de determinadas chamadas de API. Essas chamadas de API podem ter implicações, como divulgação não intencional de dados pessoais ou violações de transferências transfronteiriças específicas de dados. Por exemplo, você pode querer proibir as seguintes chamadas de API:

- Habilitação do acesso público aos buckets do Amazon Simple Storage Service (Amazon S3)
- Desabilitar a Amazon GuardDuty ou criar regras de supressão para descobertas de exfiltração de dados, como a descoberta do Trojan:EC2/Exfiltration DNSData
- Excluindo regras de AWS WAF exfiltração de dados
- Compartilhamento público de snapshots do Amazon Elastic Block Store (Amazon EBS).

- Remoção de uma conta de membro da organização
- Desassociando o Amazon CodeGuru Reviewer de um repositório

Políticas de gerenciamento

As políticas de gerenciamento do AWS Organizations podem ajudá-lo a configurar Serviços da AWS e gerenciar centralmente seus recursos. Os tipos de política de gerenciamento que você escolhe determinam como as políticas afetam OUs as contas que as herdam. As políticas de tags são um exemplo de política de AWS Organizations gerenciamento diretamente relacionada à privacidade.

Uso das políticas de marcação

As tags são pares de valores-chave que ajudam você a gerenciar, identificar, organizar, pesquisar e filtrar AWS recursos. Pode ser útil aplicar tags que diferenciem os recursos na sua organização que lidam com dados pessoais. O uso de tags é compatível com muitas das soluções de privacidade deste guia. Por exemplo, talvez você queira aplicar uma tag que indique a classificação geral dos dados que estão sendo processados ou armazenados no recurso. Você pode escrever políticas de controle de acesso por atributo (ABAC) que limitem o acesso a recursos que têm uma tag ou um conjunto de tags específicas. Por exemplo, sua política pode especificar que o perfil `SysAdmin` não pode acessar recursos que tenham a tag `dataclassification:4`. Para obter mais informações e um tutorial, consulte Definir permissões para acessar AWS recursos com base em tags na documentação do IAM. Além disso, se sua organização usa o AWS Backup para aplicar políticas de retenção de dados amplamente em seus backups em muitas contas, você pode aplicar uma tag que coloque esse recurso dentro do escopo dessa política de backup.

As políticas de marcação ajudam você a manter as tags consistentes em toda a organização. Em uma política de marcação, você especifica regras que se aplicam aos recursos quando eles são marcados. Por exemplo, você pode exigir que os recursos sejam marcados com chaves específicas, como `DataClassification` ou `DataSteward`, e você pode especificar tratamentos de caso ou valores válidos para chaves. Você também pode usar a imposição para impedir que solicitações de marcação não compatíveis sejam concluídas.

Ao usar tags como um componente principal da sua estratégia de controle de privacidade, considere o seguinte:

- Considere as implicações de colocar dados pessoais ou outros tipos de dados sensíveis em chaves ou valores de tags. Quando você entra em contato AWS para obter assistência técnica, AWS pode analisar tags e outros identificadores de recursos para ajudar a resolver o problema.

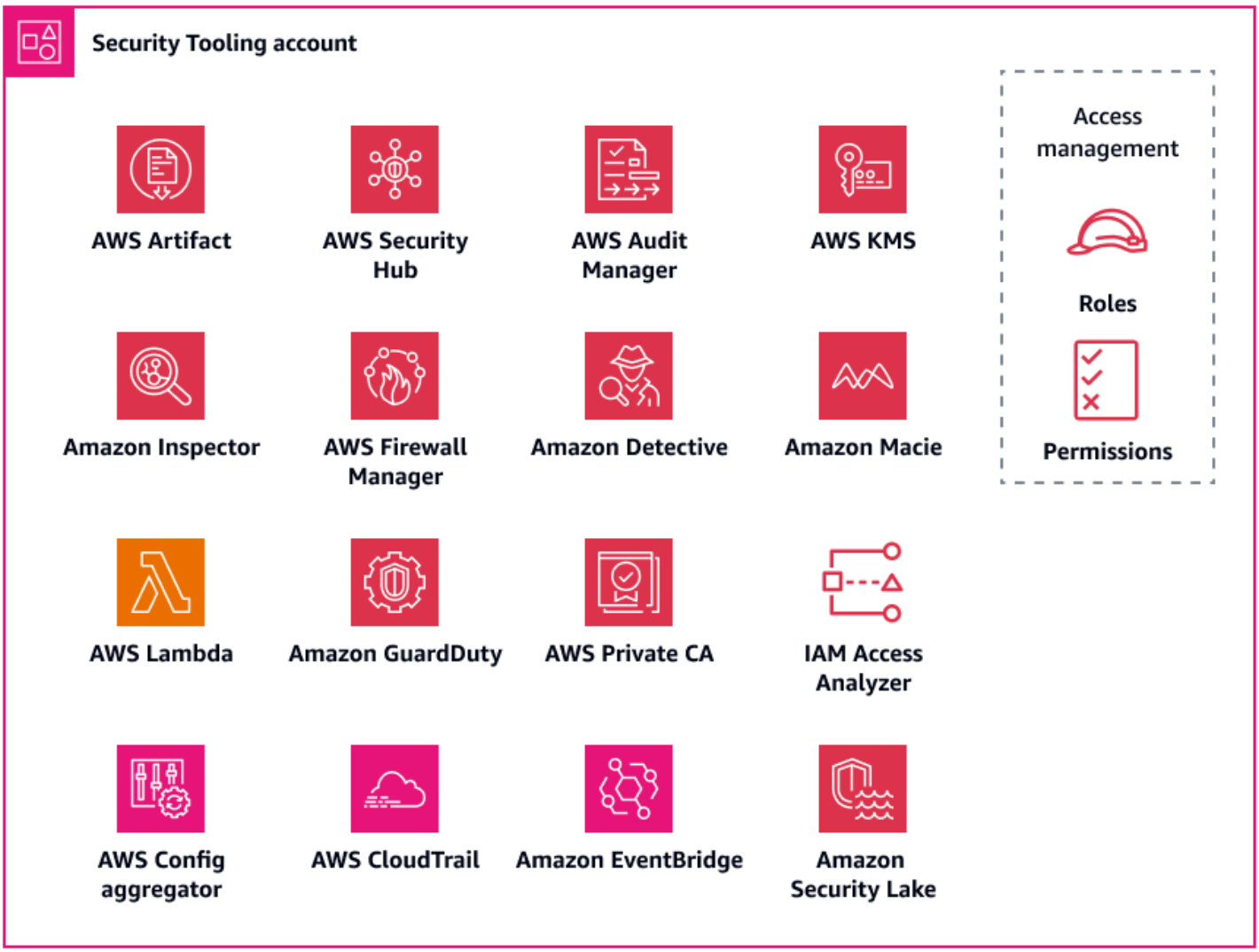
Os dados da tag não são criptografados e Serviços da AWS, por exemplo Gerenciamento de Faturamento e Custos da AWS, podem lê-los. Portanto, talvez você queira desidentificar os valores das tags e depois reidentificá-los usando um sistema que você controla, como um sistema de gerenciamento de serviços de TI (ITSM). AWS recomenda não incluir informações de identificação pessoal nas etiquetas.

- Considere que alguns valores de tags precisam ser imutáveis (não modificáveis) para evitar a evasão de controles técnicos, como condições ABAC que dependem de tags.

UO de segurança | Conta do Security Tooling

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

A conta do Security Tooling é dedicada a operar serviços básicos de segurança e privacidade Contas da AWS, monitorar e automatizar alertas e respostas de segurança e privacidade. Para obter mais informações sobre essa conta, consulte a Arquitetura AWS de Referência de Segurança (AWS SRA). O diagrama a seguir ilustra os serviços AWS de segurança e privacidade configurados na conta do Security Tooling.



Esta seção fornece informações mais detalhadas sobre o seguinte nessa conta:

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrailajuda você a auditar a atividade geral da API em seu Conta da AWS. Habilitar CloudTrail tudo Contas da AWS o Regiões da AWS que armazena, processa ou transmite dados

pessoais pode ajudá-lo a rastrear o uso e a divulgação desses dados. O AWS Security Reference Architecture recomenda habilitar uma trilha de organização, que é uma trilha única que registra em log todos os eventos de todas as contas na organização. No entanto, habilitar essa trilha da organização agrega os dados de logs de várias regiões em um único bucket do Amazon Simple Storage Service (Amazon S3) na conta do Archive Log. Para contas que lidam com dados pessoais, isso pode trazer algumas considerações adicionais de design. Os registros de log podem conter algumas referências a dados pessoais. Para atender aos requisitos de transferência e residência de dados, talvez seja necessário reconsiderar a agregação de dados de logs entre regiões em uma única região onde o bucket do S3 está localizado. Sua organização pode considerar quais workloads regionais devem ser incluídas ou excluídas da trilha organizacional. Para workloads que você decide excluir da trilha da organização, considere configurar uma trilha específica da região que mascare dados pessoais. Para obter mais informações sobre como mascarar dados pessoais, consulte a seção Amazon Data Firehose deste guia. Em última análise, sua organização pode ter uma combinação de trilhas organizacionais e trilhas regionais que se agregam à conta centralizada do Log Archive.

Para obter mais informações sobre como configurar uma trilha de região única, consulte as instruções para usar a AWS Command Line Interface (AWS CLI) ou o console. Ao criar a trilha da organização, você pode usar uma configuração de AWS Control Toweraceitação ou criar a trilha diretamente no CloudTrail console.

Para obter mais informações sobre a abordagem geral e como gerenciar a centralização de logs e os requisitos de transferência de dados, consulte a seção Armazenamento de log centralizado neste guia. Seja qual for a configuração escolhida, talvez você queira separar o gerenciamento de trilhas na conta do Security Tooling do armazenamento de registros na conta do Log Archive, de acordo com a AWS SRA. Esse design ajuda você a criar políticas de acesso com privilégio mínimo para aqueles que precisam gerenciar logs e para aqueles que precisam usar os dados de logs.

AWS Config

O AWS Config oferece uma exibição detalhada dos recursos em sua Conta da AWS e como eles são configurados. Ele ajuda você a identificar como os recursos estão relacionados entre si e como suas configurações foram alteradas ao longo do tempo. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Em AWS Config, você pode implantar pacotes de conformidade, que são conjuntos de AWS Config regras e ações de remediação. Os pacotes de conformidade fornecem uma estrutura de uso geral projetada para permitir verificações de governança de privacidade, segurança, operação e

otimização de custos usando regras gerenciadas ou personalizadas. AWS Config Você pode usar essa ferramenta como parte de um conjunto maior de ferramentas de automação para controlar se suas configurações de AWS recursos estão em conformidade com seus próprios requisitos de estrutura de controle.

O pacote de conformidade de Boas Práticas Operacionais para o NIST Privacy Framework v1.0 está alinhado a uma série de controles relacionados à privacidade do NIST Privacy Framework. Cada AWS Config regra se aplica a um tipo de AWS recurso específico e está relacionada a um ou mais controles do NIST Privacy Framework. Você pode usar esse pacote de conformidade para monitorar a conformidade contínua relacionada à privacidade em todos os recursos de suas contas. Confira abaixo algumas das regras incluídas neste pacote de conformidade:

- `no-unrestricted-route-to-igw`: esta regra ajuda a evitar a exfiltração de dados no plano de dados monitorando continuamente as tabelas de rotas da VPC em busca de rotas de saída padrão `0.0.0.0/0` ou `::/0` para um gateway da internet. Isso ajuda você a restringir para onde o tráfego vinculado à internet pode ser enviado, especialmente se houver intervalos de CIDR conhecidos por serem maliciosos.
- `encrypted-volumes`: esta regra verifica se os volumes do Amazon Elastic Block Store (Amazon EBS) que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) estão criptografados. Se sua organização tiver requisitos de controle específicos relacionados ao uso de chaves AWS Key Management Service (AWS KMS) para proteção de dados pessoais, você poderá especificar uma chave específica IDs como parte da regra para verificar se os volumes estão criptografados com uma AWS KMS chave específica.
- `restricted-common-ports`: esta regra verifica se os grupos de segurança do Amazon EC2 permitem tráfego TCP irrestrito para portas especificadas. Os grupos de segurança podem ajudá-lo a gerenciar o acesso à rede fornecendo filtragem de estado do tráfego de entrada e saída da rede para os recursos. AWS Bloquear o tráfego de entrada de `0.0.0.0/0` para portas comuns, como TCP 3389 e TCP 21, em seus recursos ajuda a restringir o acesso remoto.

AWS Config pode ser usado para verificações de conformidade proativas e reativas de seus AWS recursos. Além de considerar as regras encontradas nos pacotes de conformidade, você pode incorporá-las nos modos de avaliação de detecção e proativa. Isso ajuda a implementar verificações de privacidade mais cedo em seu ciclo de vida de desenvolvimento de software, pois os desenvolvedores de aplicações podem começar a incorporar verificações de pré-implantação. Por exemplo, eles podem incluir ganchos em seus AWS CloudFormation modelos que verificam o recurso declarado no modelo em relação a todas as AWS Config regras relacionadas à privacidade

que têm o modo proativo ativado. Para obter mais informações, consulte AWS Config Rules Now Support Proactive Compliance (publicação AWS no blog).

Amazon GuardDuty

AWS oferece vários serviços que podem ser usados para armazenar ou processar dados pessoais, como Amazon S3, Amazon Relational Database Service (Amazon RDS) ou Amazon EC2 com Kubernetes. A Amazon GuardDuty combina visibilidade inteligente com monitoramento contínuo para detectar indicadores que possam estar relacionados à divulgação não intencional de dados pessoais. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Com GuardDuty, você pode identificar atividades potencialmente maliciosas relacionadas à privacidade em todo o ciclo de vida de um ataque. Por exemplo, GuardDuty pode alertá-lo sobre conexões com sites na lista negra, tráfego de portas de rede ou volumes de tráfego incomuns, exfiltração de DNS, lançamentos inesperados de instâncias do EC2 e chamadas incomuns de ISP. Você também pode configurar GuardDuty para interromper alertas de endereços IP confiáveis de suas próprias listas de IP confiáveis e alertar sobre endereços IP maliciosos conhecidos de suas próprias listas de ameaças.

Conforme recomendado no AWS SRA, você pode habilitar GuardDuty para todos Contas da AWS em sua organização e configurar a conta do Security Tooling como administrador GuardDuty delegado. GuardDutyagrega descobertas de toda a organização em uma única conta. Para obter mais informações, consulte Gerenciando GuardDuty contas com AWS Organizations. Você também pode considerar identificar todas as partes interessadas relacionadas à privacidade no processo de resposta a incidentes, da detecção e análise à contenção e erradicação, e envolvê-las em quaisquer incidentes que possam envolver a exfiltração de dados.

IAM Access Analyzer

Muitos clientes querem garantia contínua de que os dados pessoais estão sendo compartilhados adequadamente com processadores terceirizados pré-aprovados e pretendidos, e nenhuma outra entidade. Um perímetro de dados é um conjunto de barreiras de proteção preventivas projetado para garantir que apenas identidades confiáveis das redes esperadas acessem recursos confiáveis em seu ambiente da AWS . Ao definir controles para a divulgação não intencional e intencional de dados pessoais, você pode definir identidades confiáveis, recursos confiáveis e redes esperadas.

Com o AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), as organizações podem definir uma Conta da AWS zona de confiança e configurar alertas para

violações dessa zona de confiança. O analisador de acesso do IAM analisa as políticas do IAM para ajudar a identificar e resolver o acesso público não intencional ou entre contas a recursos potencialmente sensíveis. O analisador de acesso do IAM usa lógica matemática e inferência para gerar descobertas abrangentes para recursos que podem ser acessados de fora de uma Conta da AWS. Por fim, para responder e remediar políticas excessivamente permissivas do IAM, você pode usar o analisador de acesso do IAM para validar as políticas existentes em relação às práticas recomendadas do IAM e fornecer sugestões. O analisador de acesso do IAM pode gerar uma política do IAM com privilégio mínimo baseada na atividade de acesso anterior de uma entidade principal do IAM. Ele analisa os CloudTrail registros e gera uma política que concede somente as permissões necessárias para continuar executando essas tarefas.

Para obter mais informações sobre como o analisador de acesso do IAM é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Amazon Macie

O Amazon Macie é um serviço que usa machine learning e correspondência de padrões para descobrir dados sensíveis, fornece visibilidade dos riscos de segurança de dados e ajuda você a automatizar proteções contra esses riscos. O Macie gera descobertas quando detecta possíveis violações de política ou problemas com a segurança ou privacidade dos seus buckets do Amazon S3. O Macie é outra ferramenta que as organizações podem usar para implementar a automação a fim de apoiar os esforços de conformidade. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

O Macie pode detectar uma lista grande e crescente de tipos de dados sensíveis, incluindo informações de identificação pessoal (PII), como nomes, endereços e outros atributos identificáveis. Você pode até mesmo criar identificadores de dados personalizados para definir critérios de detecção que reflitam a definição de dados pessoais da sua organização.

À medida que sua organização define controles preventivos para seus buckets do Amazon S3 que contêm dados pessoais, você pode usar o Macie como um mecanismo de validação para fornecer garantia contínua de onde seus dados pessoais estão e como estão protegidos. Para começar, habilite o Macie e configure a descoberta automatizada de dados sensíveis. O Macie analisa continuamente os objetos em todos os seus buckets do S3, em todas as contas e. Regiões da AWS O Macie gera e mantém um mapa de calor interativo que mostra onde os dados pessoais residem. O recurso automatizado de descoberta de dados sensíveis foi projetado para reduzir custos e minimizar a necessidade de configurar manualmente as tarefas de descoberta. Você pode aproveitar o recurso automatizado de descoberta de dados sensíveis e usar o Macie para detectar automaticamente

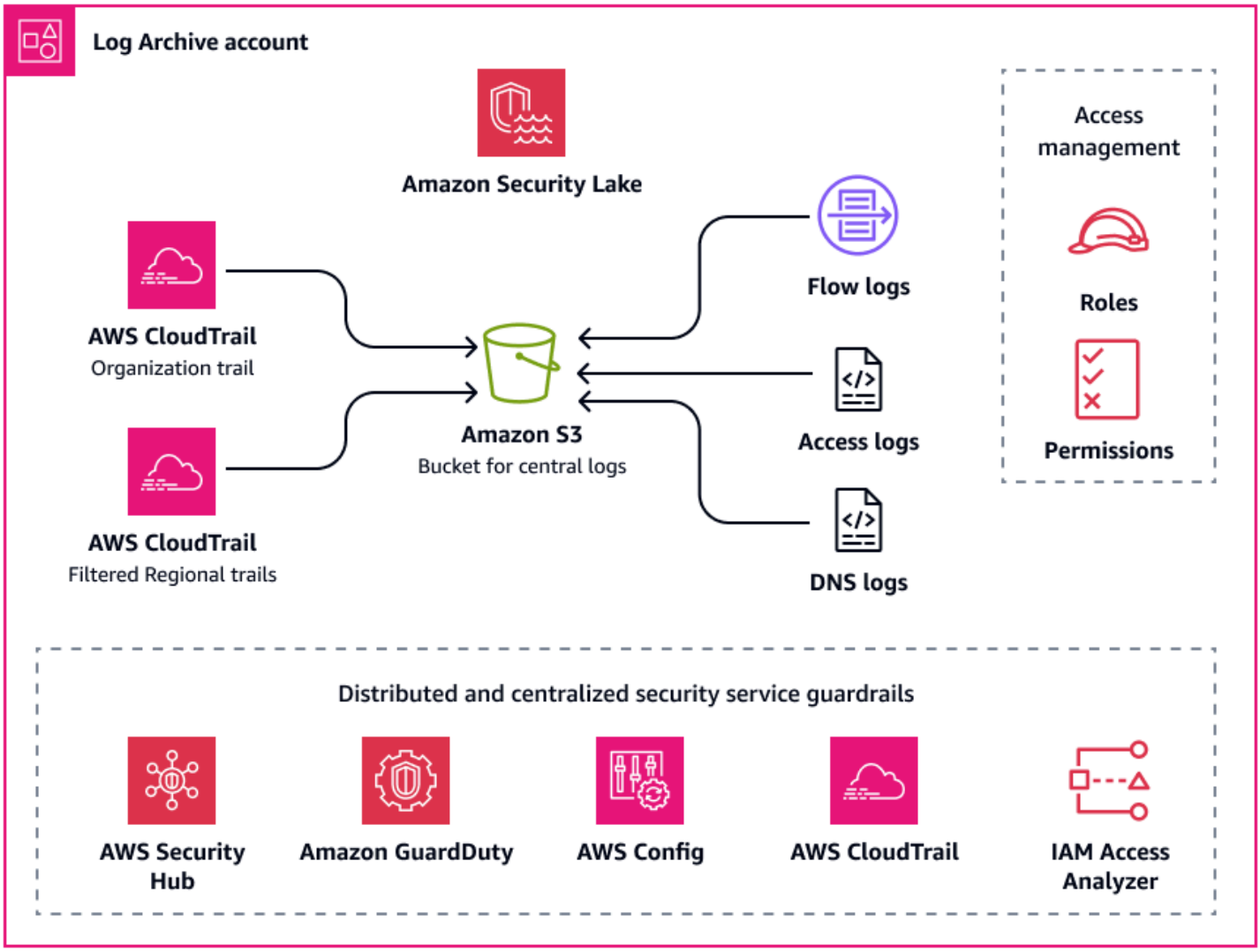
novos buckets ou novos dados em buckets existentes e, em seguida, validar os dados com base nas tags de classificação de dados atribuídas. Configure essa arquitetura para notificar as equipes apropriadas de desenvolvimento e privacidade sobre buckets classificados incorretamente ou não classificados em tempo hábil.

Você pode habilitar o Macie para cada conta em sua organização usando o. AWS Organizations Para obter mais informações, consulte Integrating and configuring an organization in Amazon Macie.

UO de segurança | Conta do Log Archive

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

A conta do Log Archive é onde você centraliza os tipos de logs de infraestrutura, serviços e aplicações. Para obter mais informações sobre essa conta, consulte a Arquitetura AWS de Referência de Segurança (AWS SRA). Com uma conta dedicada para logs, você pode aplicar alertas consistentes em todos os tipos de logs e confirmar que os agentes de resposta a incidentes podem acessar um conjunto desses logs em um só lugar. Você também pode configurar controles de segurança e políticas de retenção de dados em um só lugar, o que pode simplificar a sobrecarga operacional de privacidade. O diagrama abaixo ilustra os serviços de segurança e privacidade da AWS configurados na conta do Log Archive.



Armazenamento de log centralizado

Arquivos de log (como AWS CloudTrail registros) podem conter informações que podem ser consideradas dados pessoais. Algumas organizações optam por usar uma trilha organizacional para agregar CloudTrail registros entre Regiões da AWS contas em um local central, para fins de visibilidade. Para obter mais informações, consulte AWS CloudTrail neste guia. Ao implementar a centralização de CloudTrail registros, os registros normalmente são armazenados em um bucket do Amazon Simple Storage Service (Amazon S3) em uma única região.

Dependendo da definição de dados pessoais de sua organização, de suas obrigações contratuais com seus clientes e dos regulamentos de privacidade regionais aplicáveis, talvez seja necessário considerar transferências de dados transfronteiriças quando se tratar de agregação de logs. Determine se os dados pessoais nos vários tipos de logs se enquadram nessas restrições. Por

exemplo, CloudTrail os registros podem conter dados de funcionários de sua organização, mas podem não conter dados pessoais de seus clientes. Se sua organização precisar aderir aos requisitos restritos de transferência de dados, as seguintes opções podem oferecer apoio a essa questão:

- Se sua organização estiver fornecendo serviços Nuvem AWS para titulares de dados em vários países, você pode optar por agregar todos os registros no país que tenha os requisitos de residência de dados mais rigorosos. Por exemplo, se você estiver operando na Alemanha e ela tiver os requisitos mais rigorosos, você pode agregar dados em um bucket do S3 para que `eu-central-1` Região da AWS os dados coletados na Alemanha não saiam das fronteiras da Alemanha. Para essa opção, você pode configurar uma única trilha organizacional CloudTrail que agregue registros de todas as contas e Regiões da AWS da região de destino.
- Redija os dados pessoais que precisam permanecer Região da AWS antes de serem copiados e agregados em outra região. Por exemplo, você pode mascarar os dados pessoais na região host da aplicação antes de transferir os logs para uma região diferente. Para obter mais informações sobre como mascarar dados pessoais, consulte a seção Amazon Data Firehose deste guia.
- Se você tiver preocupações rigorosas com a soberania de dados, poderá manter uma landing zone separada com várias contas que imponha esses requisitos Região da AWS . Dessa forma, você pode simplificar a configuração da zona de pouso na região para o registro em log centralizado. Ela também fornece vantagens adicionais de segregação de infraestrutura e ajuda a manter o log local em sua própria região. Trabalhe com seu advogado para determinar quais dados pessoais estão no escopo e quais Region-to-Region transferências são permitidas. Para obter mais informações, consulte Elaboração de estratégias para uma expansão global neste guia.

Por meio de registros de serviços, registros de aplicativos e registros do sistema operacional (SO), você pode usar CloudWatch a Amazon para monitorar Serviços da AWS nossos recursos em sua conta e região correspondentes por padrão. Muitos optam por centralizar esses logs e métricas de várias contas e regiões em uma única conta. Por padrão, esses logs persistem na conta correspondente e na região de origem. Para centralização, você pode usar filtros de assinatura e tarefas de exportação do Amazon S3 para compartilhar dados em um local centralizado. Talvez seja importante incluir os filtros e as tarefas de exportação adequados ao agregar logs de uma workload que tenha requisitos de transferência de dados transfronteiriça. Se os logs de acesso de uma workload contiverem dados pessoais, talvez seja necessário garantir que eles sejam transferidos ou retidos em contas e regiões específicas.

Amazon Security Lake

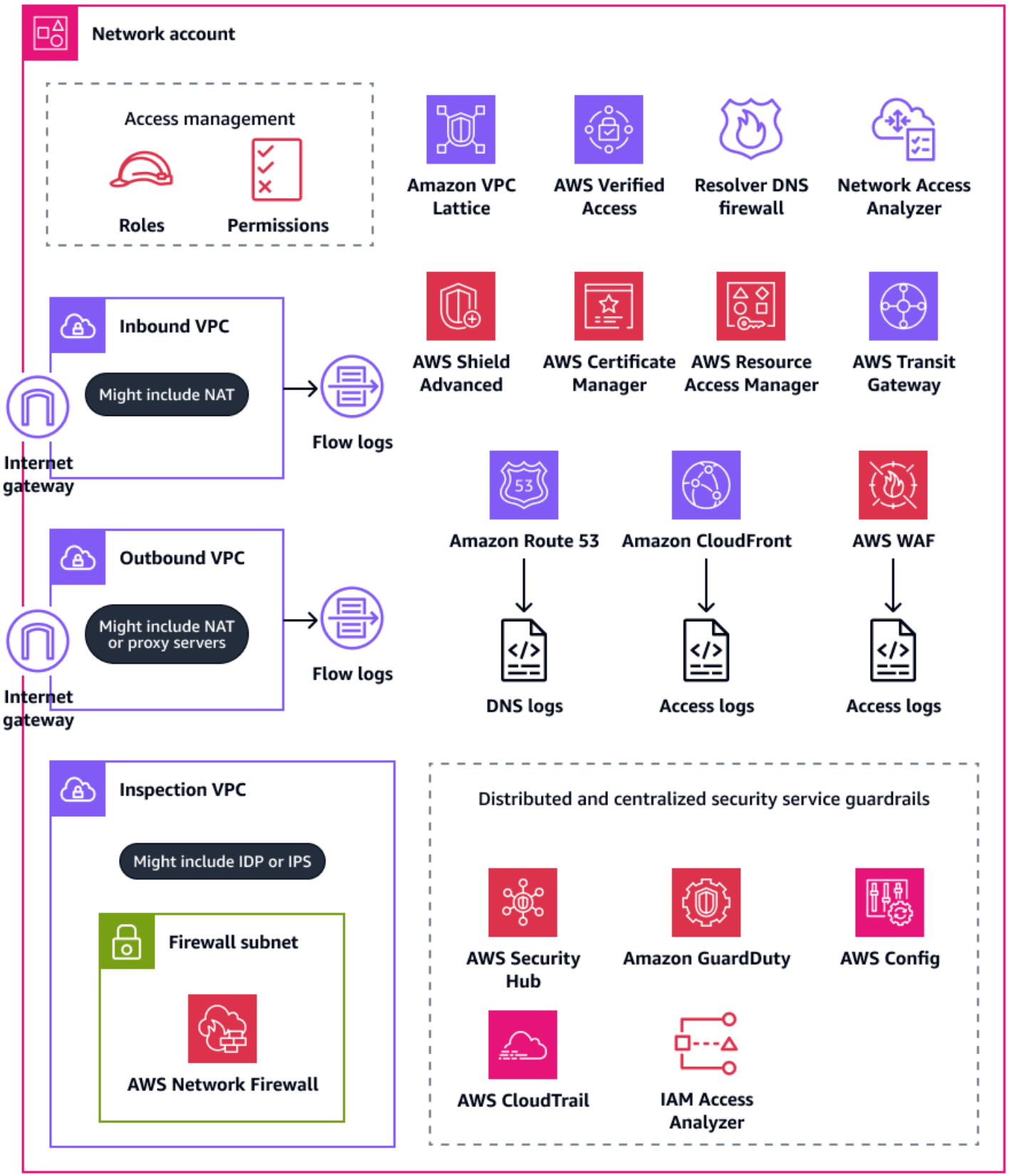
Conforme recomendado no AWS SRA, talvez você queira usar a conta do Log Archive como a conta de administrador delegado do Amazon Security Lake. Quando você faz isso, o Security Lake coleta logs compatíveis em buckets dedicados do Amazon S3 na mesma conta que outros logs de segurança recomendados pelo SRA.

Do ponto de vista da privacidade, é importante que seus respondentes a incidentes tenham acesso aos registros de seus AWS ambientes, provedores de SaaS, locais, fontes na nuvem e fontes de terceiros. Isso os ajuda a bloquear e remediar mais rapidamente o acesso não autorizado aos dados pessoais. As mesmas considerações sobre o armazenamento de logs provavelmente se aplicam à residência de logs e à movimentação regional dentro do Amazon Security Lake. Isso ocorre porque o Security Lake coleta registros e eventos de segurança do local Regiões da AWS em que você ativou o serviço. Para cumprir os requisitos de residência de dados, considere sua configuração de regiões de rollup.Uma região de rollup é uma região em que o Security Lake consolida dados de uma ou mais regiões contribuintes, que você seleciona. Talvez sua organização precise se alinhar aos requisitos regionais de conformidade para a residência de dados antes que você possa configurar o Security Lake e regiões de rollup.

Infraestrutura de UO: conta de Rede

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Na conta Rede, você gerencia a rede entre suas nuvens privadas virtuais (VPCs) e a Internet em geral. Nessa conta, você pode implementar amplos mecanismos de controle de divulgação usando AWS WAF, use AWS Resource Access Manager (AWS RAM) para compartilhar sub-redes e AWS Transit Gateway anexos de VPC e usar a CloudFront Amazon para oferecer suporte ao uso direcionado de serviços. Para obter mais informações sobre essa conta, consulte a Arquitetura AWS de Referência de Segurança (AWS SRA). O diagrama a seguir ilustra os serviços de AWS segurança e privacidade configurados na conta de rede.


Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Esta seção fornece informações mais detalhadas sobre os seguintes Serviços da AWS que são usados nessa conta:

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

A Amazon CloudFront oferece suporte a restrições geográficas para aplicativos de front-end e hospedagem de arquivos. CloudFrontpode fornecer conteúdo por meio de uma rede mundial de data centers chamados de pontos de presença. Quando um usuário solicita o conteúdo com o qual você está servindo CloudFront, a solicitação é encaminhada para o ponto de presença que fornece a menor latência. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Atualmente, seu programa de privacidade pode oferecer suporte à conformidade com leis regionais específicas. Se sua workload tiver como escopo fornecer serviços somente a clientes que residem apenas nessas regiões, você poderá implementar medidas técnicas que impeçam o uso de outras regiões. Você pode usar restrições CloudFront geográficas para impedir que usuários em localizações geográficas específicas acessem o conteúdo que você está distribuindo por meio de uma CloudFront distribuição. Para obter mais informações e opções de configuração para restrições geográficas, consulte Restringir a distribuição geográfica do seu conteúdo na CloudFront documentação.

Você também pode configurar CloudFront para gerar registros de acesso que contêm informações detalhadas sobre cada solicitação de usuário CloudFront recebida. Para obter mais informações, consulte Configuração e uso de registros padrão (registros de acesso) na CloudFront documentação. Por fim, se CloudFront estiver configurado para armazenar em cache o conteúdo em uma série de pontos de presença, você pode considerar onde ocorre o armazenamento em cache. Para algumas organizações, o armazenamento em cache entre regiões pode estar sujeito aos requisitos de transferência de dados transfronteiriças.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar seus recursos com segurança Contas da AWS para reduzir a sobrecarga operacional e fornecer visibilidade e

auditabilidade. Com AWS RAM, as organizações podem restringir quais AWS recursos podem ser compartilhados com outras Contas da AWS pessoas da organização ou com contas de terceiros. Para obter mais informações, consulte AWS Recursos compartilháveis. Na conta de rede, você pode usar AWS RAM para compartilhar sub-redes VPC e conexões de gateway de trânsito. Se você costuma AWS RAM compartilhar uma conexão de plano de dados com outra pessoa Conta da AWS, considere estabelecer processos para verificar se as conexões são feitas de acordo com os requisitos de residência de dados pré-aprovadas Regiões da AWS e cumprem seus requisitos de residência de dados.

Além das conexões de gateway de compartilhamento VPCs e trânsito, AWS RAM pode ser usado para compartilhar recursos que não oferecem suporte às políticas baseadas em recursos do IAM. Para uma carga de trabalho hospedada na UO de Dados Pessoais, você pode usar AWS RAM para acessar dados pessoais localizados em uma área separada Conta da AWS. Para obter mais informações, consulte AWS Resource Access Manager na seção UO de dados pessoais | Conta do PD Application.

AWS Transit Gateway

Se você quiser implantar AWS recursos que coletem, armazenem ou processem Regiões da AWS dados pessoais de acordo com seus requisitos de residência de dados organizacionais e tiver as proteções técnicas apropriadas, considere a implementação de grades de proteção para evitar fluxos de dados transfronteiriços não aprovados nos planos de controle e de dados. No ambiente de gerenciamento, você pode limitar o uso da região e, como resultado, os fluxos de dados entre regiões usando políticas de controle de serviços e do IAM.

Há várias opções para controlar fluxos de dados entre regiões no plano de dados. Por exemplo, você pode usar tabelas de rotas, emparelhamento de VPC e anexos. AWS Transit Gateway AWS Transit Gatewayé um hub central que conecta nuvens privadas virtuais (VPCs) e redes locais. Como parte de sua AWS landing zone maior, você pode considerar as várias maneiras pelas quais os dados podem ser percorridos Regiões da AWS, inclusive por meio de gateways de Internet, por meio de peering direto e por meio de VPC-to-VPC peering entre regiões com. AWS Transit Gateway Por exemplo, você pode fazer o seguinte no AWS Transit Gateway:

- Confirme se as conexões leste-oeste e norte-sul entre seus ambientes VPCs e locais estão alinhadas com seus requisitos de privacidade.
- Definir as configurações da VPC de acordo com seus requisitos de privacidade.
- Use uma política de controle de serviços AWS Organizations e políticas do IAM para ajudar a evitar modificações nas suas configurações AWS Transit Gateway e nas da Amazon Virtual Private

Cloud (Amazon VPC). Para ver um exemplo de política de controle de serviços, consulte Restringir as alterações nas configurações da VPC neste guia.

AWS WAF

Para ajudar a evitar a divulgação não intencional de dados pessoais, você pode implantar uma defense-in-depth abordagem para seus aplicativos da web. Você pode criar validação de entrada e limitação de taxa em seu aplicativo, mas AWS WAF pode servir como outra linha de defesa. AWS WAFé um firewall de aplicativo web que ajuda você a monitorar solicitações HTTP e HTTPS que são encaminhadas para seus recursos protegidos de aplicativos web. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

Com AWS WAF, você pode definir e implantar regras que inspecionam critérios específicos. As seguintes atividades podem estar associadas à divulgação não intencional de dados pessoais:

- Tráfego proveniente de endereços IP ou localizações geográficas desconhecidas ou maliciosas.
- Os dez principais ataques do Open Worldwide Application Security Project (OWASP), incluindo ataques relacionados à exfiltração, como injeção de SQL
- Altas taxas de solicitações
- Tráfego geral de bots
- Extratores de conteúdo

Você pode implantar grupos de AWS WAF regras que são gerenciados pelo AWS. Alguns grupos de regras gerenciados do AWS WAF podem ser usados para detectar ameaças à privacidade e aos dados pessoais, por exemplo:

- Banco de dados SQL: este grupo de regras contém regras para bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção de SQL. Considere usar esse grupo de regras se sua aplicação se conectar com um banco de dados SQL.
- Entradas ruins conhecidas: este grupo de regras contém regras para bloquear padrões de solicitação conhecidos como inválidos e associados à exploração ou à descoberta de vulnerabilidades.
- Controle de bots: este grupo de regras contém regras criadas para gerenciar solicitações de bots, que podem consumir recursos em excesso, distorcer as métricas de negócios, causar tempo de inatividade e realizar atividades maliciosas.

- Prevenção contra apropriação de contas (ATP): este grupo de regras contém regras criadas para evitar tentativas mal-intencionadas de invasão de contas. Este grupo de regras inspeciona as tentativas de login enviadas para o endpoint de login da sua aplicação.

UO de dados pessoais | Conta do PD Application

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

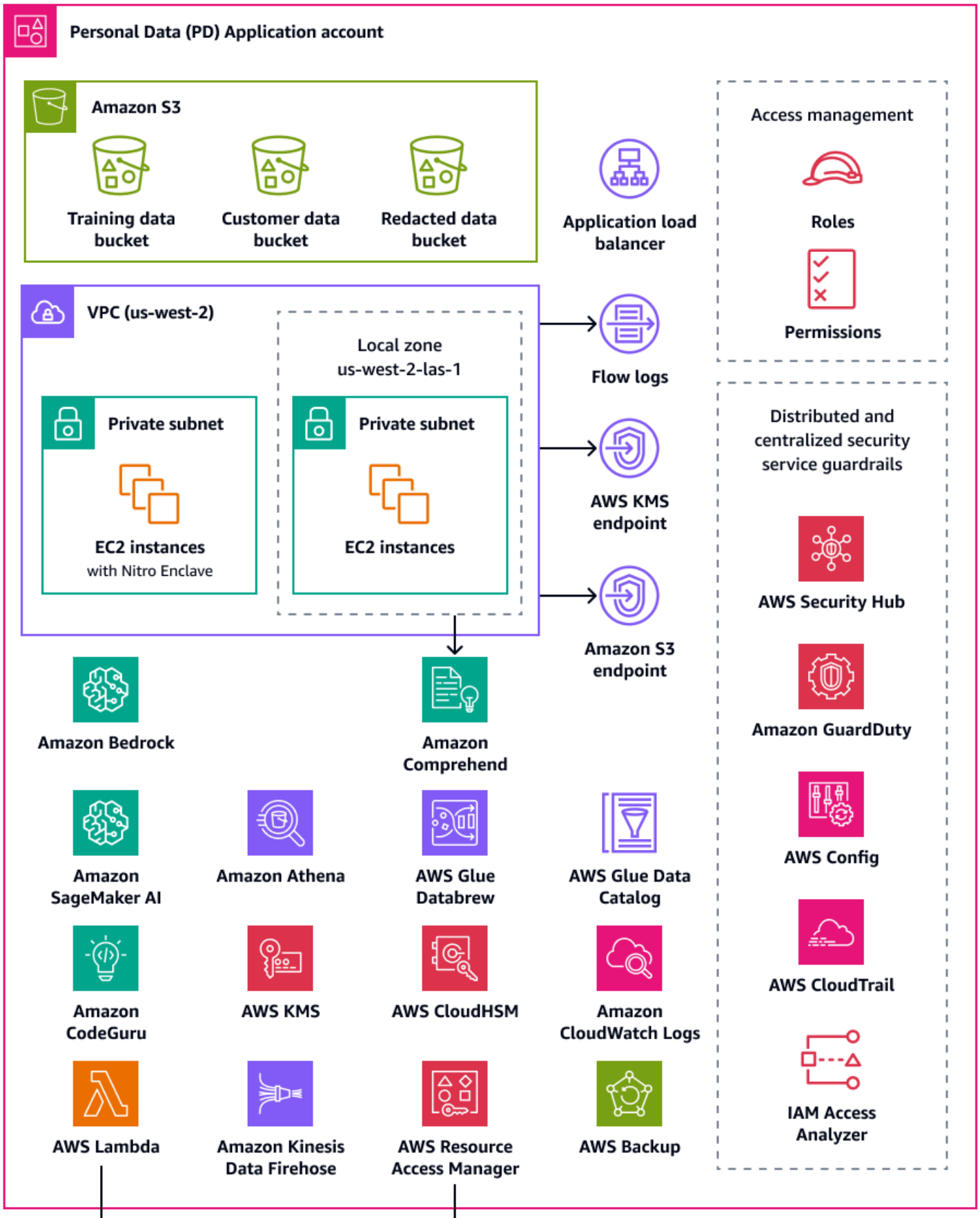
A conta do Personal Data (PD) Application é onde sua organização hospeda serviços que coletam e processam dados pessoais. Especificamente, você pode armazenar o que você define como dados pessoais nessa conta. O AWS PRA demonstra vários exemplos de configurações de privacidade por meio de uma arquitetura web sem servidor de várias camadas. Quando se trata de operar cargas de trabalho em um AWS landing zone, as configurações de privacidade não devem ser consideradas one-size-fits-all soluções. Por exemplo, seu objetivo pode ser entender os conceitos subjacentes, como eles podem melhorar a privacidade e como sua organização pode aplicar soluções aos seus casos de uso e arquiteturas específicos.

Pois Contas da AWS em sua organização que coleta, armazena ou processa dados pessoais, você pode usar AWS Organizations e AWS Control Tower implantar proteções básicas e reproduzíveis. Estabelecimento de uma unidade organizacional (UO) dedicada para essas contas é fundamental. Por exemplo, você talvez queira aplicar barreiras de proteção de residência de dados somente a um subconjunto de contas em que a residência de dados é uma consideração fundamental do design. Para muitas organizações, estas são as contas que armazenam e processam dados pessoais.

Sua organização pode considerar oferecer suporte a uma conta de dados dedicada, que é onde você armazena a fonte autorizada de seus conjuntos de dados pessoais. Uma fonte de dados autorizada é um local onde você armazena a versão primária dos dados, que pode ser considerada a versão mais confiável e precisa dos dados. Por exemplo, você pode copiar os dados da fonte de dados autorizada para outros locais, como buckets do Amazon Simple Storage Service (Amazon S3) na conta do PD Application que são usados para armazenar dados de treinamento, um subconjunto de dados do cliente e dados ocultados. Ao adotar essa abordagem de várias contas para separar conjuntos de dados pessoais completos e definitivos na conta de dados das workloads downstream

do consumidor na conta do PD Application, você pode reduzir o escopo do impacto no caso de acesso não autorizado às suas contas.

O diagrama a seguir ilustra os serviços de AWS segurança e privacidade configurados nas contas de aplicativos e dados do PD.


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Access management

Esta seção fornece informações mais detalhadas sobre os seguintes Serviços da AWS que são usados nessas contas:

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- CloudWatch Registros da Amazon
- CodeGuru Revisor da Amazon
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- Zonas locais da AWS
- AWS Enclaves Nitro
- AWS PrivateLink
- AWS Resource Access Manager
- SageMaker IA da Amazon
- AWS recursos que ajudam a gerenciar o ciclo de vida dos dados
- Serviços da AWS e recursos que ajudam a segmentar dados
- Serviços da AWS e recursos que ajudam a descobrir, classificar ou catalogar dados

Amazon Athena

Você pode considerar os controles de limitação de consultas de dados para atender às suas metas de privacidade. O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon S3 usando SQL padrão. Você não precisa carregar os dados no Athena. Ele funciona diretamente com os dados armazenados nos buckets do S3.

Um caso de uso comum do Athena é fornecer às equipes de data analytics conjuntos de dados personalizados e limpos. Se os conjuntos de dados contiverem dados pessoais, você poderá limpar o conjunto de dados mascarando colunas inteiras de dados pessoais que fornecem pouco valor às

equipes de data analytics. Para obter mais informações, consulte Anonimizar e gerenciar dados em seu data lake com o Amazon Athena AWS Lake Formation e AWS (postagem no blog).

Se sua abordagem de transformação de dados exigir flexibilidade adicional fora das funções com suporte no Athena, você poderá definir funções personalizadas denominadas funções definidas pelo usuário (UDF). Você pode invocar UDFs em uma consulta SQL enviada ao Athena e elas são executadas em. AWS Lambda Você pode usar `FILTER` `SQL` consultas UDFs in `SELECT` e pode invocar várias UDFs na mesma consulta. Para fins de privacidade, você pode criar UDFs tipos específicos de mascaramento de dados, como mostrar somente os últimos quatro caracteres de cada valor em uma coluna.

Amazon Bedrock

O Amazon Bedrock é um serviço totalmente gerenciado que fornece acesso aos modelos básicos das principais empresas de IA, como AI21 Labs, Anthropic, Meta, Mistral AI e Amazon. Ele ajuda as organizações a criar e escalar aplicações de IA generativa. Independentemente da plataforma usada, ao usar a IA generativa, as organizações podem enfrentar riscos de privacidade, incluindo a possível exposição de dados pessoais, acesso não autorizado a dados e outras violações de conformidade.

As Barreiras de Proteção para Amazon Bedrock foram projetadas para ajudar a mitigar esses riscos aplicando as práticas recomendadas de segurança e conformidade em todas as suas workloads de IA generativa no Amazon Bedrock. A implantação e o uso de recursos de IA nem sempre estão alinhados aos requisitos de privacidade e conformidade de uma organização. As organizações podem ter dificuldade em manter a privacidade dos dados ao usar modelos de IA generativa porque esses modelos podem provavelmente memorizar ou reproduzir informações confidenciais. As Barreiras de Proteção para Amazon Bedrock ajudam a proteger a privacidade avaliando as entradas do usuário e as respostas do modelo. No geral, se os dados de entrada contiverem dados pessoais, poderá haver o risco de essas informações serem expostas na saída do modelo.

As Barreiras de Proteção para Amazon Bedrock fornecem mecanismos para aplicar políticas de proteção de dados e ajudar a evitar a exposição não autorizada de dados. Elas oferecem recursos de filtragem de conteúdo para detectar e bloquear dados pessoais nas entradas, restrições de tópicos para ajudar a impedir o acesso a assuntos impróprios ou arriscados e filtros de palavras para mascarar ou ocultar termos sensíveis nos prompts e respostas do modelo. Esses recursos ajudam a evitar eventos que podem levar a violações de privacidade, como respostas tendenciosas ou a perda gradual da confiança do cliente. Esses recursos podem ajudar você a garantir que os dados pessoais não sejam processados ou divulgados inadvertidamente pelos seus modelos de IA. As

Barreiras de Proteção para Amazon Bedrock também são compatíveis com a avaliação de entradas e respostas fora do Amazon Bedrock. Para obter mais informações, consulte Implement model-independent safety measures with Amazon Bedrock Guardrails (publicação do Blog da AWS).

Com as Barreiras de Proteção para Amazon Bedrock, você pode limitar o risco de alucinações em modelos usando verificações de fundamentação contextual, que avaliam a fundamentação factual e a relevância das respostas. Um exemplo é a implantação de uma aplicação de IA generativa voltada para o cliente que usa fontes de dados de terceiros em uma aplicação de geração aumentada via recuperação (RAG). As verificações de fundamentação contextual podem ser usadas para validar as respostas do modelo em relação a essas fontes de dados e a filtrar respostas imprecisas. No contexto do AWS PRA, você pode implementar o Amazon Bedrock Guardrails em todas as contas de carga de trabalho, onde ele impõe proteções de privacidade específicas que são adaptadas aos requisitos de cada carga de trabalho.

AWS Clean Rooms

À medida que as organizações buscam maneiras de colaborar umas com as outras por meio da análise de conjuntos de dados confidenciais que se cruzam ou se sobrepõem, manter a segurança e a privacidade desses dados compartilhados é uma preocupação. O AWS Clean Rooms ajuda você a implantar salas limpas de dados, que são ambientes seguros e neutros em que as organizações podem analisar conjuntos de dados combinados sem compartilhar os dados brutos em si. Ele também pode gerar insights exclusivos ao fornecer acesso a outras organizações AWS sem mover ou copiar dados de suas próprias contas e sem revelar o conjunto de dados subjacente. Todos os dados permanecem no local de origem. As regras de análise integradas restringem a saída e as consultas SQL. Todas as consultas são registradas em log, e os membros de colaboração podem ver como seus dados estão sendo consultados.

Você pode criar uma AWS Clean Rooms colaboração e convidar outros AWS clientes para serem membros dessa colaboração. Você concede a um membro a capacidade de consultar os conjuntos de dados de membros, e você pode escolher membros adicionais para receber os resultados dessas consultas. Se mais de um membro precisar consultar os conjuntos de dados, você poderá criar colaborações adicionais com as mesmas fontes de dados e configurações de membros diferentes. Cada membro pode filtrar os dados que são compartilhados com os membros da colaboração, e você pode usar regras de análise personalizadas para definir limitações sobre como os dados que eles fornecem à colaboração podem ser analisados.

Além de restringir os dados apresentados à colaboração e como eles podem ser usados por outros membros, AWS Clean Rooms fornece os seguintes recursos que podem ajudar você a proteger a privacidade:

- A privacidade diferencial é uma técnica matemática que aprimora a privacidade do usuário adicionando uma quantidade cuidadosamente calibrada de ruído aos dados. Isso ajuda a reduzir o risco de reidentificação individual do usuário no conjunto de dados sem obscurecer os valores de interesse. Usar a privacidade diferencial do AWS Clean Rooms não exige experiência em privacidade diferencial.
- O AWS Clean Rooms ML permite que duas partes identifiquem usuários semelhantes em seus dados sem a necessidade de compartilhar dados diretamente entre si. Isso reduz o risco de ataques de inferência de membros, em que um membro da colaboração pode identificar indivíduos no conjunto de dados do outro membro. Ao criar um modelo semelhante e gerar um segmento semelhante, o AWS Clean Rooms ML ajuda você a comparar conjuntos de dados sem expor os dados originais. Isso não exige que nenhum dos membros tenha experiência em ML ou realize qualquer trabalho fora do AWS Clean Rooms. Você mantém total controle e propriedade do modelo treinado.
- A computação criptográfica para o Clean Rooms (C3R) pode ser usada com regras de análise para obter insights de dados confidenciais. Ela limita criptograficamente o que qualquer outra parte da colaboração pode saber. Usando o cliente de criptografia C3R, os dados são criptografados no cliente antes de serem fornecidos. AWS Clean Rooms Como as tabelas de dados são criptografadas usando uma ferramenta de criptografia do lado do cliente antes de serem carregadas no Amazon S3, os dados permanecem criptografados e persistem durante o processamento.

No AWS PRA, recomendamos que você crie AWS Clean Rooms colaborações na conta de dados. Você pode usá-las para compartilhar dados criptografados de clientes com terceiros. Use-as somente quando houver uma sobreposição nos conjuntos de dados fornecidos. Para obter mais informações sobre como determinar a sobreposição, consulte Regra de análise de lista na AWS Clean Rooms documentação.

CloudWatch Registros da Amazon

O Amazon CloudWatch Logs ajuda você a centralizar os registros de todos os seus sistemas e aplicativos, Serviços da AWS para que você possa monitorá-los e arquivá-los com segurança. Em CloudWatch Registros, você pode usar uma política de proteção de dados para grupos de registros novos ou existentes para ajudar a minimizar o risco de divulgação de dados pessoais. As políticas de

proteção de dados podem detectar dados sensíveis, como dados pessoais, em seus logs. A política de proteção de dados pode mascarar esses dados quando os usuários acessam os logs por meio do Console de gerenciamento da AWS. Quando os usuários precisam de acesso direto aos dados pessoais, de acordo com a especificação geral da finalidade da sua workload, você pode atribuir permissões `logs:Unmask` para esses usuários. Você também pode criar uma política de proteção de dados para toda a conta e aplicar essa política de forma consistente em todas as contas da sua organização. Isso configura o mascaramento por padrão para todos os grupos de registros atuais e futuros no CloudWatch Logs. Também recomendamos que você habilite os relatórios de auditoria e os envie para outro grupo de logs, um bucket do Amazon S3 ou o Amazon Data Firehose. Esses relatórios contêm um registro detalhado das descobertas de proteção de dados em cada grupo de logs.

CodeGuru Revisor da Amazon

Tanto para a privacidade quanto para a segurança, é vital para muitas organizações que elas ofereçam suporte à conformidade contínua durante as fases de implantação e pós-implantação. O AWS PRA inclui controles proativos nos pipelines de implantação de aplicações que processam dados pessoais. O Amazon CodeGuru Reviewer pode detectar possíveis defeitos que possam expor dados pessoais em código Java e JavaScript Python. Ele oferece sugestões aos desenvolvedores para melhorar o código. CodeGuru O revisor pode identificar defeitos em uma ampla variedade de práticas gerais recomendadas de segurança, privacidade e. Ele foi projetado para funcionar com vários provedores de origem AWS CodeCommit, incluindo Bitbucket e Amazon S3. GitHub Alguns dos defeitos relacionados à privacidade que o CodeGuru Revisor pode detectar incluem:

- Injeção de SQL
- Cookies não seguros
- Autorização ausente
- Recriptografia do lado do cliente AWS KMS

Para obter uma lista completa do que o CodeGuru Reviewer pode detectar, consulte a Amazon CodeGuru Detector Library.

Amazon Comprehend

O Amazon Comprehend é um serviço de processamento de linguagem natural (PLN) que usa machine learning para descobrir insights valiosos e relações em documentos de texto em inglês. O Amazon Comprehend pode detectar e ocultar dados pessoais em documentos de texto estruturados,

semiestruturados ou não estruturados. Para obter mais informações, consulte Personally identifiable information (PII) na documentação do Amazon Comprehend.

Como o Amazon Comprehend tem muitas opções para integração de aplicativos, você pode AWS SDKs usar o Amazon Comprehend para identificar dados pessoais em vários lugares diferentes onde você coleta, armazena e processa dados. Você pode usar os recursos do Amazon Comprehend ML para detectar e editar dados pessoais em registros de aplicativos AWS (publicação no blog), e-mails de clientes, tickets de suporte e muito mais. O diagrama de arquitetura da conta do PD Application mostra como você pode executar essa função para logs de aplicações no Amazon EC2. O Amazon Comprehend oferece dois modos de ocultação:

- `REPLACE_WITH_PII_ENTITY_TYPE` substitui cada entidade de PII por seus tipos. Por exemplo, Jane Doe será substituída por NAME.
- `MASK` substitui os caracteres em entidades de PII por um caractere de sua escolha (!, #, $, %, &, ou @). Por exemplo, Jane Doe pode ser substituída por **** ***.

Amazon Data Firehose

O Amazon Data Firehose pode ser usado para capturar, transformar e carregar dados de streaming em serviços downstream, como o Amazon Managed Service for Apache Flink ou o Amazon S3. O Firehose costuma ser usado para transportar grandes quantidades de dados de streaming, como logs de aplicações, sem precisar criar pipelines de processamento do zero.

Você pode usar as funções do Lambda para realizar um processamento personalizado ou incorporado antes que os dados sejam enviados para o downstream. Para fins de privacidade, esse recurso é compatível com os requisitos de minimização de dados e transferência de dados transfronteiriças. Por exemplo, você pode usar o Lambda e o Firehose para transformar dados de logs de várias regiões antes de serem centralizados na conta do Log Archive. Para obter mais informações, consulte Biogen: solução de registro centralizada para várias contas (vídeo). YouTube Na conta do aplicativo PD, você configura AWS CloudTrail a Amazon CloudWatch e envia os registros para um stream de entrega do Firehose. Uma função do Lambda transforma os logs e os envia para um bucket central do S3 na conta do Log Archive. Você pode configurar a função do Lambda para mascarar campos específicos que contêm dados pessoais. Isso ajuda a evitar a transferência de dados pessoais nas Regiões da AWS. Ao usar essa abordagem, os dados pessoais são mascarados antes da transferência e da centralização, e não depois. Para aplicativos em jurisdições que não estão sujeitas aos requisitos de transferência internacional, normalmente é mais eficiente e econômico do ponto de vista operacional agregar registros por meio da trilha

organizacional. CloudTrail Para obter mais informações, consulte AWS CloudTrail na seção UO de segurança | Conta do Security Tooling deste guia.

Amazon DataZone

À medida que as organizações ampliam sua abordagem de compartilhamento de dados por meio Serviços da AWS de AWS Lake Formation, elas querem garantir que o acesso diferencial seja controlado por aqueles que estão mais familiarizados com os dados: os proprietários dos dados. No entanto, esses proprietários de dados podem estar cientes dos requisitos de privacidade, como consentimento ou considerações sobre transferências de dados transfronteiriças. A Amazon DataZone ajuda os proprietários de dados e a equipe de governança de dados a compartilhar e consumir dados em toda a organização de acordo com suas políticas de governança de dados. Na Amazon DataZone, as linhas de negócios (LOBs) gerenciam seus próprios dados e um catálogo rastreia essa propriedade. As partes interessadas podem encontrar e solicitar acesso aos dados como parte de suas tarefas de negócios. Desde que siga as políticas estabelecidas pelos publicadores de dados, o proprietário dos dados pode conceder acesso às tabelas subjacentes, sem um administrador ou sem transferir os dados.

Em um contexto de privacidade, a Amazon DataZone pode ser útil nos seguintes exemplos de casos de uso:

- Uma aplicação voltada para o cliente gera dados de uso que podem ser compartilhados com um LOB de marketing separado. Você precisa garantir que somente os dados dos clientes que optaram pelo marketing sejam publicados no catálogo.
- Os dados de clientes europeus são publicados, mas só podem ser assinados por pessoas LOBs locais do Espaço Econômico Europeu (EEE). Para obter mais informações, consulte Melhore a segurança dos dados com controles de acesso refinados na Amazon. DataZone

No AWS PRA, você pode conectar os dados no bucket compartilhado do Amazon S3 à Amazon DataZone como produtor de dados.

AWS Glue

A manutenção de conjuntos de dados que contêm dados pessoais é um componente essencial da Privacidade por Design. Os dados de uma organização podem existir em formas estruturadas, semiestruturadas ou não estruturadas. Conjuntos de dados pessoais sem estrutura podem dificultar a realização de várias operações de aprimoramento da privacidade, incluindo minimização de

dados, rastreamento de dados atribuídos a um único titular de dados como parte de uma solicitação do titular dos dados, garantia de qualidade consistente dos dados e segmentação geral dos conjuntos de dados. O AWS Glue é um serviço de extração, transformação e carregamento (ETL) totalmente gerenciado. Ele pode ajudá-lo a categorizar, limpar, enriquecer e mover dados entre armazenamentos de dados e fluxos de dados. AWS Glue os recursos são projetados para ajudar você a descobrir, preparar, estruturar e combinar conjuntos de dados para análise, aprendizado de máquina e desenvolvimento de aplicativos. Você pode usar AWS Glue para criar uma estrutura previsível e comum sobre seus conjuntos de dados existentes. AWS Glue Data Catalog, AWS Glue DataBrew, e Qualidade AWS Glue de dados são AWS Glue recursos que podem ajudar a suportar os requisitos de privacidade da sua organização.

AWS Glue Data Catalog

O AWS Glue Data Catalog ajuda você a estabelecer conjuntos de dados sustentáveis. O Catálogo de Dados contém referências a dados que são usados como fontes e destinos para trabalhos de extração, transformação e carregamento (ETL) em AWS Glue. As informações no Catálogo de Dados são armazenadas como tabelas de metadados, em que cada tabela especifica um único armazenamento de dados. Você executa um crawler do AWS Glue para fazer um inventário dos dados em vários tipos de armazenamento de dados. Você adiciona classificadores integrados e personalizados ao crawler, e esses classificadores inferem o formato e o esquema dos dados pessoais. O crawler então grava os metadados no Catálogo de Dados. Uma tabela de metadados centralizada pode facilitar a resposta às solicitações dos titulares dos dados (como o direito ao apagamento), pois agrega estrutura e previsibilidade em diferentes fontes de dados pessoais em seu ambiente. AWS Para obter um exemplo abrangente de como usar o catálogo de dados para responder automaticamente a essas solicitações, consulte Como lidar com solicitações de eliminação de dados em seu data lake com o Amazon S3 Find and Forget AWS (postagem no blog). Por fim, se sua organização está usando o AWS Lake Formation para administrar e fornecer acesso refinado em bancos de dados, tabelas, linhas e células, o Catálogo de Dados é um componente essencial. O Data Catalog fornece compartilhamento de dados entre contas e ajuda você a usar o controle de acesso baseado em tags para gerenciar seu data lake em grande escala (postagem noAWS blog). Para obter mais informações, consulte AWS Lake Formation nesta seção.

AWS Glue DataBrew

O AWS Glue DataBrew ajuda você a limpar e normalizar dados e pode realizar transformações nos dados, como remover ou mascarar informações de identificação pessoal e criptografar campos de dados sensíveis em pipelines de dados. Você também pode mapear visualmente a linhagem dos seus dados para entender as várias fontes de dados e as etapas de transformação pelas quais os

dados passaram. Esse recurso se torna cada vez mais importante à medida que sua organização trabalha para entender e rastrear melhor a proveniência dos dados pessoais. DataBrew ajuda você a mascarar dados pessoais durante a preparação dos dados. Você pode detectar dados pessoais como parte de um trabalho de criação de perfil de dados e coletar estatísticas, como o número de colunas que podem conter dados pessoais e categorias em potencial. Em seguida, você pode usar técnicas integradas de transformação de dados reversíveis ou irreversíveis, incluindo substituição, hashing, criptografia e decodificação, tudo isso sem escrever nenhum código. Você pode então usar os conjuntos de dados limpos e mascarados downstream para tarefas de analytics, relatórios e machine learning. Algumas das técnicas de mascaramento de dados disponíveis em DataBrew incluem:

- Hash: aplique funções de hash aos valores da coluna.
- Substituição: substitua dados pessoais por outros valores que pareçam autênticos.
- Anulação ou exclusão: substitua um campo específico por um valor nulo, ou exclua a coluna.
- Mascaramento: use o embaralhamento de caracteres ou mascare certas partes nas colunas.

Confira abaixo as técnicas de criptografia disponíveis:

- Criptografia determinística: aplique algoritmos de criptografia determinística aos valores da coluna. A criptografia determinística sempre produz o mesmo texto cifrado para um valor.
- Criptografia probabilística: aplique algoritmos de criptografia probabilística aos valores da coluna. A criptografia probabilística produz texto cifrado diferente toda vez que é aplicada.

Para obter uma lista completa das receitas de transformação de dados pessoais fornecidas em DataBrew, consulte Etapas da receita de informações de identificação pessoal (PII).

AWS Glue Qualidade de dados

AWS Glue A qualidade de dados ajuda você a automatizar e operacionalizar a entrega de dados de alta qualidade em todos os pipelines de dados, de forma proativa, antes de serem entregues aos consumidores de dados. AWS Glue O Data Quality fornece análise estatística de problemas de qualidade de dados em seus pipelines de dados, pode acionar alertas na Amazon EventBridge e fazer recomendações de regras de qualidade para remediação. AWS Glue A qualidade de dados também oferece suporte à criação de regras com uma linguagem específica do domínio para que você possa criar regras personalizadas de qualidade de dados.

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 usa módulos de segurança de hardware para proteger e validar AWS KMS keys sob o Programa de Validação de Módulos Criptográficos FIPS 140-2. Para obter mais informações sobre como esse serviço é usado em um contexto de segurança, consulte o AWS Security Reference Architecture.

AWS KMS se integra à maioria dos Serviços da AWS que oferecem criptografia, e você pode usar chaves KMS em seus aplicativos que processam e armazenam dados pessoais. Você pode usar o AWS KMS para ajudar a atender aos seus diversos requisitos de privacidade e proteger dados pessoais, incluindo:

- Usar chaves gerenciadas pelo cliente para maior controle da força, rotação, expiração e outras opções.
- Usar chaves dedicadas gerenciadas pelo cliente para proteger dados pessoais e segredos que permitem acesso a dados pessoais.
- Definir níveis de classificação de dados e designar pelo menos uma chave dedicada gerenciada pelo cliente por nível. Por exemplo, você pode ter uma chave para criptografar dados operacionais e outra para criptografar dados pessoais.
- Impedir acesso não intencional entre contas a chaves do KMS.
- Armazenar chaves KMS dentro do Conta da AWS mesmo recurso a ser criptografado.
- Implementar a separação de tarefas para a administração e o uso de chaves do KMS. Para obter mais informações, consulte Como usar o KMS e o IAM para habilitar controles de segurança independentes para dados criptografados no S3 (postagem do AWS blog).
- Impor a rotação automática de chaves por meio de barreiras de proteção preventivas e reativas.

Por padrão, as chaves do KMS são armazenadas e podem ser usadas somente na região em que foram criadas. Se sua organização tem requisitos específicos de residência e soberania de dados, considere se as chaves de várias regiões do KMS são apropriadas para seu caso de uso. As chaves multirregionais são chaves KMS para fins especiais Regiões da AWS que podem ser usadas de forma intercambiável. O processo de criação de uma chave multirregional move seu material de chave além das Região da AWS fronteiras internas AWS KMS, portanto, essa falta de isolamento regional pode não ser compatível com as metas de soberania e residência de sua organização. Uma forma de resolver essa questão é usar um tipo diferente de chave do KMS, como uma chave gerenciada pelo cliente específica da região.

Armazenamentos de chaves externas

Para muitas organizações, o armazenamento de AWS KMS chaves padrão no Nuvem AWS pode atender à soberania de dados e aos requisitos regulamentares gerais. Mas alguns podem exigir que as chaves de criptografia sejam criadas e mantidas fora de um ambiente de nuvem e que você tenha caminhos de autorização e auditoria independentes. Com os armazenamentos de chaves externos AWS KMS, você pode criptografar dados pessoais com material chave que sua organização possui e controla fora do Nuvem AWS. Você ainda interage com a AWS KMS API normalmente, mas AWS KMS interage somente com o software proxy externo de armazenamento de chaves (proxy XKS) fornecido por você. Seu proxy externo de armazenamento de chaves então medeia toda a comunicação entre AWS KMS e seu gerenciador de chaves externo.

Ao usar um repositório de chaves externo para criptografia de dados, é importante considerar a sobrecarga operacional adicional em comparação com a manutenção das chaves do AWS KMS. Com um repositório de chaves externo, é necessário criar, configurar e manter o repositório de chaves externo. Além disso, se houver erros na infraestrutura adicional que você deve manter, como o proxy XKS, e a conectividade for perdida, os usuários poderão ficar temporariamente impossibilitados de descriptografar e acessar os dados. Trabalhe em estreita colaboração com suas partes interessadas em conformidade e regulamentação para entender as obrigações legais e contratuais da criptografia de dados pessoais e seus contratos de nível de serviço para disponibilidade e resiliência.

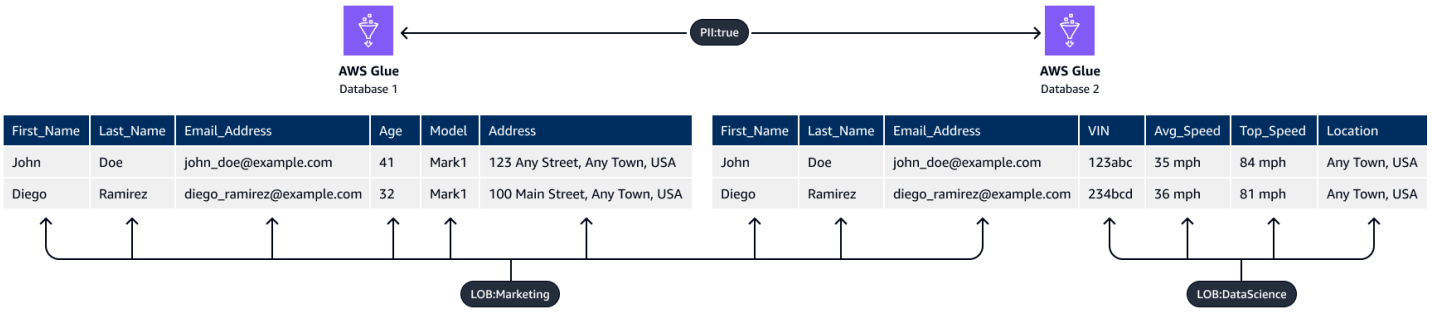
AWS Lake Formation

Muitas organizações que catalogam e categorizam seus conjuntos de dados por meio de catálogos estruturados de metadados desejam compartilhar esses conjuntos de dados em toda a organização. Você pode usar políticas de permissão AWS Identity and Access Management (IAM) para controlar o acesso a conjuntos de dados inteiros, mas geralmente é necessário um controle mais granular para conjuntos de dados que contêm dados pessoais de sensibilidade variável. Por exemplo, a especificação da finalidade e a limitação de uso (site do FPC) podem indicar que uma equipe de marketing precisa acessar os endereços dos clientes, mas uma equipe de ciência de dados não.

Também há desafios de privacidade associados aos data lakes, que centralizam o acesso a grandes quantidades de dados sensíveis em seu formato original. A maioria dos dados de uma organização pode ser acessada de forma centralizada em um só lugar, portanto, a separação lógica dos conjuntos de dados, especialmente aqueles que contêm dados pessoais, pode ser fundamental. O AWS Lake Formation pode ajudar você a configurar a governança e o monitoramento ao compartilhar dados, sejam eles de uma única fonte ou de várias fontes contidas em um data lake. No

AWS PRA, você pode usar o Lake Formation para fornecer controle de acesso refinado aos dados no bucket de dados compartilhado na conta de dados.

Você pode usar o recurso de controle de acesso baseado em tags no Lake Formation. O controle de acesso baseado em tags é uma estratégia de autorização que define permissões com base em atributos. No Lake Formation, esses atributos são chamados de tags do LF. Usando uma tag LF, você pode anexar essas tags aos bancos de dados, tabelas e colunas do Catálogo de Dados e conceder as mesmas tags às entidades principais do IAM. O Lake Formation permite operações nesses recursos quando a entidade principal teve o acesso concedido a um valor de tag que corresponde ao valor da tag do recurso. A imagem a seguir mostra como você pode atribuir tags LF e permissões para fornecer acesso diferenciado aos dados pessoais.



Este exemplo usa a natureza hierárquica das tags. Ambos os bancos de dados contêm informações de identificação pessoal (`PII:true`), mas as tags no nível colunar limitam colunas específicas a equipes diferentes. Neste exemplo, os diretores do IAM que têm a `PII:true` tag LF podem acessar os recursos do AWS Glue banco de dados que têm essa tag. As entidades principais com a tag LF `LOB:DataScience` podem acessar colunas específicas que têm essa tag, e as entidades principais com a tag LF `LOB:Marketing` podem acessar somente as colunas que têm essa tag. O marketing pode acessar somente as PII relevantes para os casos de uso de marketing, e a equipe de ciência de dados pode acessar somente as PII relevantes para seus casos de uso.

Zonas locais da AWS

Se precisar cumprir os requisitos de residência de dados, você pode implantar recursos que armazenam e processam dados pessoais de forma específica Regiões da AWS para dar suporte a esses requisitos. Você também pode usar Zonas locais da AWS, o que ajuda a colocar computação, armazenamento, banco de dados e outros AWS recursos selecionados perto de grandes centros populacionais e setoriais. Uma zona local é uma extensão de uma Região da AWS que está na proximidade geográfica de uma grande área metropolitana. Você pode colocar tipos específicos de recursos em uma zona local, perto da região à qual a zona local corresponde. As zonas locais podem ajudar você a atender aos requisitos de residência de dados quando uma região não está

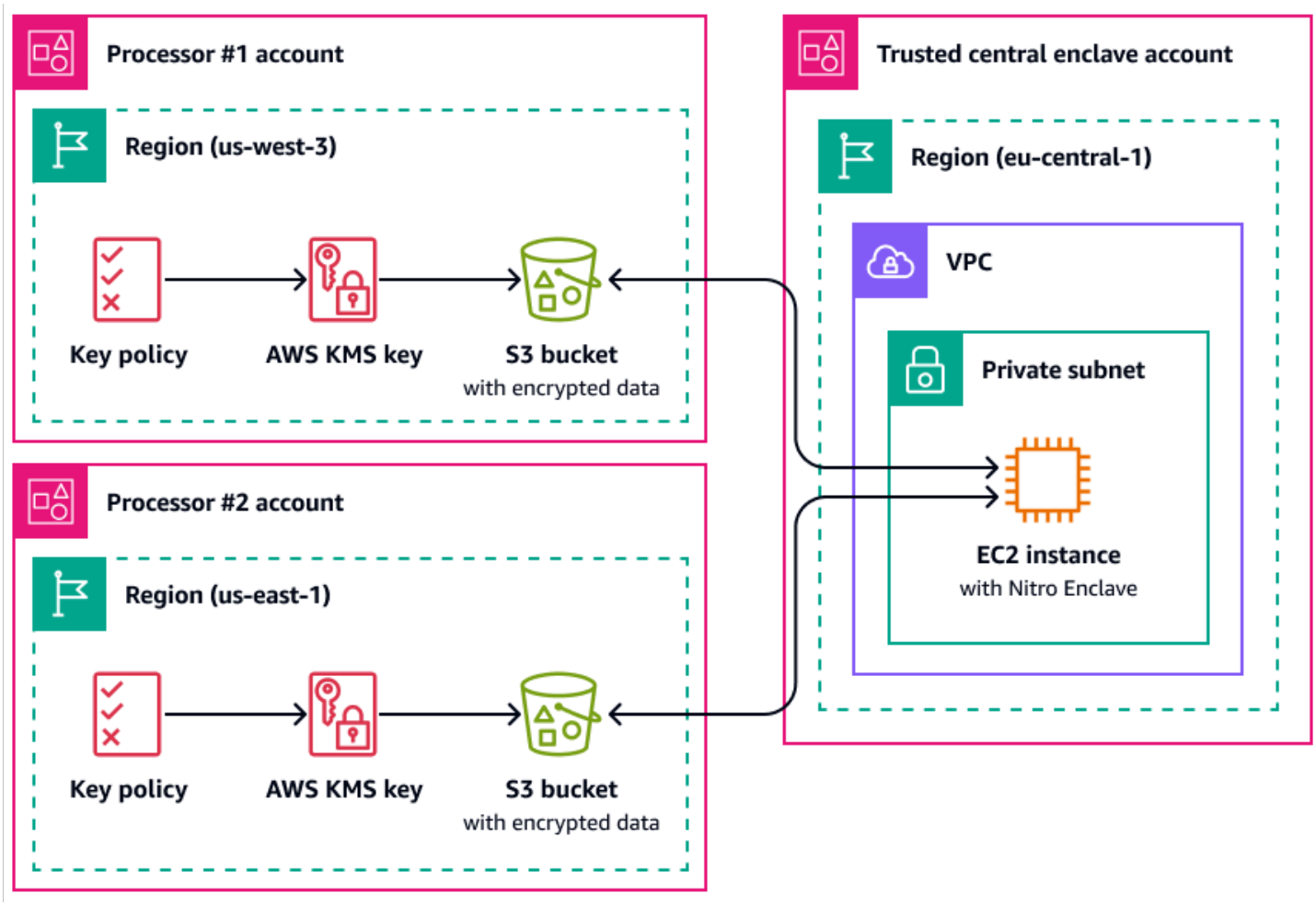
disponível na mesma jurisdição legal. Ao usar zonas locais, considere os controles de residência de dados implantados em sua organização. Por exemplo, você pode precisar de um controle para evitar transferências de dados de uma zona local específica para outra região. Para obter mais informações sobre como usar SCPs para manter as grades de proteção de transferência de dados transfronteiriças, consulte Melhores práticas para gerenciar a residência de dados no uso de controles de landing Zonas locais da AWS zone (AWS postagem no blog).

AWS Enclaves Nitro

Considere sua estratégia de segmentação de dados de uma perspectiva de processamento, como processamento de dados pessoais com um serviço de computação, como o Amazon Elastic Compute Cloud (Amazon EC2). A computação confidencial como parte de uma estratégia de arquitetura maior pode ajudar a isolar o processamento de dados pessoais em um enclave de CPU isolado, protegido e confiável. Os enclaves são máquinas virtuais separadas, reforçadas e altamente restritas. AWS Nitro Enclaves é um recurso do Amazon EC2 que pode ajudar você a criar esses ambientes computacionais isolados. Para obter mais informações, consulte O design de segurança do sistema AWS Nitro (AWS white paper).

O Nitro Enclaves implementa um kernel separado do kernel da instância principal. O kernel da instância principal não tem acesso ao enclave. Os usuários não podem usar SSH ou acessar remotamente os dados e aplicações no enclave. As aplicações que processam dados pessoais podem ser incorporados ao enclave e configurados para usar o Vsock do enclave, o soquete que facilita a comunicação entre o enclave e a instância principal.

Um caso de uso em que o Nitro Enclaves pode ser útil é o processamento conjunto entre dois processadores de dados que estão separados Regiões da AWS e que podem não confiar um no outro. A imagem a seguir mostra como você pode usar um enclave para processamento central, uma chave do KMS para criptografar os dados pessoais antes de serem enviados ao enclave e uma política de AWS KMS key que verifica se o enclave que está solicitando a descriptografia tem as medidas exclusivas em seu documento de atestado. Para obter mais informações e instruções, consulte Usando o atestado criptográfico com. AWS KMS Para ver um exemplo de política de chave, consulte Exigir atestado para usar uma chave AWS KMS neste guia.



Com essa implementação, somente os respectivos processadores de dados e o enclave subjacente têm acesso aos dados pessoais em texto simples. O único lugar onde os dados são expostos, fora dos ambientes dos respectivos processadores de dados, é no próprio enclave, projetado para impedir o acesso e a adulteração.

AWS PrivateLink

Muitas organizações querem limitar a exposição de dados pessoais a redes não confiáveis. Por exemplo, se você quiser aprimorar a privacidade do design geral da arquitetura do aplicativo, poderá segmentar redes com base na sensibilidade dos dados (semelhante à separação lógica e física dos conjuntos de dados discutida na Serviços da AWS e recursos que ajudam a segmentar dados seção). AWS PrivateLinkajuda você a criar conexões unidirecionais e privadas de suas nuvens privadas virtuais (VPCs) para serviços fora da VPC. Usando o AWS PrivateLink, você pode configurar conexões privadas dedicadas aos serviços que armazenam ou processam dados pessoais em seu ambiente. Não há necessidade de se conectar a endpoints públicos e transferir esses dados por redes públicas não confiáveis. Quando você ativa pontos de extremidade de

AWS PrivateLink serviço para os serviços dentro do escopo, não há necessidade de um gateway de internet, dispositivo NAT, endereço IP público, AWS Direct Connect conexão ou AWS Site-to-Site VPN conexão para se comunicar. Ao se conectar AWS PrivateLink a um serviço que fornece acesso a dados pessoais, você pode usar políticas de endpoint de VPC e grupos de segurança para controlar o acesso, de acordo com a definição do perímetro de dados da sua organização. Para ver um exemplo de política de VPC endpoint que permite que somente os princípios e AWS recursos do IAM em uma organização confiável acessem um endpoint de serviço, consulte Exigir associação à organização para acessar os recursos da VPC este guia.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar seus recursos com segurança Contas da AWS para reduzir a sobrecarga operacional e fornecer visibilidade e auditabilidade. Ao planejar sua estratégia de segmentação de várias contas, considere usar AWS RAM para compartilhar os armazenamentos de dados pessoais que você armazena em uma conta separada e isolada. Você pode compartilhar esses dados pessoais com outras contas confiáveis para fins de processamento. Em AWS RAM, você pode gerenciar permissões que definem quais ações podem ser executadas em recursos compartilhados. Todas as chamadas de API para AWS RAM estão logadas CloudTrail. Além disso, você pode configurar o Amazon CloudWatch Events para notificá-lo automaticamente sobre eventos específicos AWS RAM, como quando são feitas alterações em um compartilhamento de recursos.

Embora você possa compartilhar muitos tipos de AWS recursos com outras pessoas Contas da AWS usando políticas baseadas em recursos no IAM ou políticas de bucket no Amazon S3 AWS RAM , oferece vários benefícios adicionais para a privacidade. AWS fornece aos proprietários de dados visibilidade adicional sobre como e com quem os dados são compartilhados entre você Contas da AWS, incluindo:

- Ser capaz de compartilhar um recurso com uma OU inteira em vez de atualizar manualmente as listas de contas IDs
- Aplicação do processo de convite para iniciar o compartilhamento se a conta do consumidor não fizer parte da sua organização
- Visibilidade de quais entidades principais específicas do IAM têm acesso a cada recurso individual

Se você já usou uma política baseada em recursos para gerenciar um compartilhamento de recursos e quiser usá-la AWS RAM em vez disso, use a operação da PromoteResourceShareCreatedFromPolicyAPI.

SageMaker IA da Amazon

O Amazon SageMaker AI é um serviço gerenciado de aprendizado de máquina (ML) que ajuda você a criar e treinar modelos de ML e depois implantá-los em um ambiente hospedado pronto para produção. SageMaker A IA foi projetada para facilitar a preparação de dados de treinamento e a criação de recursos de modelo.

Monitor de SageMaker modelo Amazon

Muitas organizações consideram o desvio de dados ao treinar modelos de ML. Um desvio de dados é 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. Se a natureza estatística dos dados que o modelo de ML recebe durante a produção se desviar da natureza dos dados da linha de base em que foi treinado, a precisão de suas predições pode diminuir. O Amazon SageMaker Model Monitor pode monitorar continuamente a qualidade dos modelos de aprendizado de máquina de SageMaker IA da Amazon em produção e monitorar a qualidade dos dados. A detecção antecipada e proativa do desvio de dados pode ajudar a implementar ações corretivas, como modelos de reciclagem, auditoria de sistemas upstream ou correção de problemas de qualidade de dados. O Model Monitor pode aliviar a necessidade de monitorar modelos manualmente ou criar ferramentas adicionais.

Amazon SageMaker Clarify

O Amazon SageMaker Clarify fornece uma visão sobre o viés e a explicabilidade do modelo. SageMaker O Clarify é comumente usado durante a preparação dos dados do modelo de ML e na fase geral de desenvolvimento. Os desenvolvedores podem especificar atributos de interesse, como sexo ou idade, e o SageMaker Clarify executa um conjunto de algoritmos para detectar qualquer presença de viés nesses atributos. Depois que o algoritmo é executado, o SageMaker Clarify fornece um relatório visual com uma descrição das fontes e medidas de possíveis distorções para que você possa identificar as etapas para remediar a distorção. Por exemplo, em um conjunto de dados financeiros que contém apenas alguns exemplos de empréstimos comerciais para uma faixa etária em comparação com outras, SageMaker poderia sinalizar desequilíbrios para que você possa evitar um modelo que desfavoreça essa faixa etária. Você também pode verificar se há viés em modelos já treinados revisando suas predições e monitorando continuamente esses modelos de ML em busca de viés. Por fim, o SageMaker Clarify é integrado ao Amazon SageMaker AI Experiments para fornecer um gráfico que explica quais recursos contribuíram mais para o processo geral de previsão de um modelo. Essas informações podem ser úteis para obter resultados de explicabilidade, e

podem ajudar a determinar se uma entrada específica do modelo tem mais influência do que deveria no comportamento geral do modelo.

Cartão SageMaker modelo Amazon

O Amazon SageMaker Model Card pode ajudá-lo a documentar detalhes críticos sobre seus modelos de ML para fins de governança e emissão de relatórios. Esses detalhes podem incluir o proprietário do modelo, o propósito geral, os casos de uso pretendidos, suposições feitas, classificação de risco de um modelo, detalhes e métricas de treinamento e resultados da avaliação. Para obter mais informações, consulte Explicabilidade do modelo com soluções de inteligência AWS artificial e aprendizado de máquina (AWS whitepaper).

Amazon SageMaker Data Wrangler

O Amazon SageMaker Data Wrangler é uma ferramenta de aprendizado de máquina que ajuda a otimizar o processo de preparação de dados e engenharia de recursos. Ele fornece uma interface visual que ajuda cientistas de dados e engenheiros de machine learning a preparar e transformar dados de forma rápida e fácil para uso em modelos de machine learning. Com o Data Wrangler, você pode importar dados de várias fontes, como Amazon S3, Amazon Redshift e Amazon Athena. Em seguida, você pode usar mais de 300 transformações de dados integradas para limpar, normalizar e combinar atributos sem precisar escrever nenhum código.

O Data Wrangler pode ser usado como parte do processo de preparação de dados e engenharia de recursos no PRA AWS . Ele suporta criptografia de dados em repouso e em trânsito usando AWS KMS, e usa funções e políticas do IAM para controlar o acesso a dados e recursos. Ele suporta o mascaramento de dados por meio da AWS Glue Amazon SageMaker Feature Store. Se você integrar o Data Wrangler com AWS Lake Formation, poderá aplicar controles e permissões de acesso a dados refinados. Você pode até mesmo usar o Data Wrangler com o Amazon Comprehend para ocultar automaticamente dados pessoais de dados tabulares como parte de seu fluxo de trabalho mais amplo de operações de ML. Para obter mais informações, consulte Editar automaticamente PII para aprendizado de máquina usando o Amazon SageMaker Data Wrangler (AWS postagem no blog).

A versatilidade do Data Wrangler ajuda você a mascarar dados sensíveis de muitos setores, como números de contas, números de cartão de crédito, números de previdência social, nomes de pacientes e registros médicos e militares. Você pode limitar o acesso a quaisquer dados sensíveis ou optar por ocultá-los.

AWS recursos que ajudam a gerenciar o ciclo de vida dos dados

Quando os dados pessoais não são mais necessários, você pode usar o ciclo de vida e as time-to-live políticas para dados em vários armazenamentos de dados diferentes. Ao configurar políticas de retenção de dados, considere os seguintes locais que podem conter dados pessoais:

- Bancos de dados, como o Amazon DynamoDB e o Amazon Relational Database Service (Amazon RDS)
- Buckets do Amazon S3
- Registros de CloudWatch e CloudTrail
- Dados em cache de migrações em AWS Database Migration Service (AWS DMS) e projetos AWS Glue DataBrew
- Backups e snapshots

O seguinte Serviços da AWS e os recursos a seguir podem ajudá-lo a configurar políticas de retenção de dados em seus AWS ambientes:

- Amazon S3 Lifecycle: um conjunto de regras que define as ações que o Amazon S3 aplica a um grupo de objetos. Na configuração do Amazon S3 Lifecyle, você pode criar ações de expiração, que definem quando o Amazon S3 exclui objetos expirados em seu nome. Para obter mais informações, consulte Gerenciar seu ciclo de vida de armazenamento.
- Amazon Data Lifecycle Manager — No Amazon EC2, crie uma política que automatize a criação, retenção e exclusão de snapshots do Amazon Elastic Block Store (Amazon EBS) e Amazon Machine Images () apoiados pelo EBS. AMIs
- Tempo de vida (TTL) do Amazon DynamoDB: define um carimbo por item que determina quando um item não é mais necessário. Pouco depois da data e hora do carimbo especificado, o DynamoDB exclui o item da tabela.
- Configurações de retenção de CloudWatch registros em Registros — Você pode ajustar a política de retenção de cada grupo de registros para um valor entre 1 dia e 10 anos.
- AWS Backup— implante centralmente políticas de proteção de dados para configurar, gerenciar e governar sua atividade de backup em uma variedade de AWS recursos, incluindo buckets S3, instâncias de banco de dados RDS, tabelas do DynamoDB, volumes do EBS e muito mais. Aplique políticas de backup aos seus AWS recursos especificando os tipos de recursos ou forneça granularidade adicional aplicando com base nas tags de recursos existentes. Audite e gere

relatórios sobre a atividade de backup em um console centralizado para ajudar a atender aos requisitos de conformidade de backup.

Serviços da AWS e recursos que ajudam a segmentar dados

A segmentação de dados é o processo pelo qual você armazena dados em contêineres separados. Isso pode ajudar você a fornecer medidas diferenciadas de segurança e autenticação para cada conjunto de dados e a reduzir o escopo do impacto da exposição em seu conjunto de dados geral. Por exemplo, em vez de armazenar todos os dados do cliente em um grande banco de dados, você pode segmentar esses dados em grupos menores e mais gerenciáveis.

Você pode usar a separação física e lógica para segmentar dados pessoais:

- Separação física: o ato de armazenar dados em armazenamentos de dados separados ou distribuí-los em recursos da AWS separados. Embora os dados estejam fisicamente separados, os dois recursos podem estar acessíveis para as mesmas entidades principais. É por isso que recomendamos combinar separação física com separação lógica.
- Separação lógica: o ato de isolar dados usando controles de acesso. Diferentes funções de trabalho exigem diferentes níveis de acesso a subconjuntos de dados pessoais. Para conferir um exemplo de política que implementa a separação lógica, consulte Conceder acesso a atributos específicos do Amazon DynamoDB neste guia.

A combinação de uma separação lógica e física fornece flexibilidade, simplicidade e granularidade ao escrever políticas baseadas em identidade e recursos para oferecer suporte ao acesso diferenciado em todas as funções de trabalho. Por exemplo, pode ser operacionalmente complexo criar políticas que separem logicamente diferentes classificações de dados em um único bucket do S3. O uso de buckets do S3 dedicados para cada classificação de dados simplifica a configuração e o gerenciamento de políticas.

Serviços da AWS e recursos que ajudam a descobrir, classificar ou catalogar dados

Algumas organizações ainda não começaram a usar ferramentas de extração, transformação e carregamento (ETL) em seu ambiente para catalogar proativamente seus dados. Esses clientes podem estar em um estágio inicial de descoberta de dados, em que desejam entender melhor os dados que armazenam e processam AWS e como eles são estruturados e classificados. Você pode usar o Amazon Macie para entender melhor seus dados de PII no Amazon S3. No entanto, o

Amazon Macie não pode ajudar você a analisar outras fontes de dados, como o Amazon Relational Database Service (Amazon RDS) e o Amazon Redshift. Você pode usar duas abordagens para acelerar a descoberta inicial no começo de um exercício maior de mapeamento de dados:

- Abordagem manual: crie uma tabela com duas colunas e quantas linhas você precisar. Na primeira coluna, escreva uma caracterização de dados (como nome de usuário, endereço ou sexo) que pode estar no cabeçalho ou no corpo de um pacote de rede ou em qualquer serviço que você forneça. Peça à sua equipe de conformidade que preencha a segunda coluna. Na segunda coluna, insira “sim” se os dados forem considerados pessoais e “não” se não forem. Indique qualquer tipo de dado pessoal considerado particularmente sensível, como denominação religiosa ou dados de saúde.
- Abordagem automatizada: use as ferramentas fornecidas por meio do AWS Marketplace. Uma dessas ferramentas é a Securiti. Essas soluções oferecem integrações que permitem digitalizar e descobrir dados em vários tipos de recursos da AWS , bem como ativos em outras plataformas de serviços em nuvem. Muitas dessas mesmas soluções podem coletar e manter continuamente um inventário de ativos de dados e atividades de processamento de dados em um catálogo de dados centralizado. Se você depende de uma ferramenta para realizar a classificação automatizada, talvez seja necessário ajustar as regras de descoberta e classificação para se alinhar à definição de dados pessoais da sua organização.

Exemplos de políticas relacionadas à privacidade

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Muitas organizações que lidam com dados sensíveis adotam uma abordagem preventiva, com camadas de controles reativos e de detecção implementados em toda a estrutura. Esta seção fornece exemplos de políticas relacionadas à privacidade para AWS Identity and Access Management (IAM) AWS Organizations, e AWS Key Management Service ().AWS KMS Essas políticas podem ajudar sua organização a atingir várias metas de privacidade de uso, limitação de divulgação e transferência de dados transfronteiriça usando uma abordagem preventiva. Muitas dessas políticas foram referenciadas nas seções anteriores deste guia.

Esta seção contém os seguintes exemplos de políticas:

- Exigir acesso de endereços IP específicos
- Exigir associação à organização para acessar os recursos da VPC
- Restrinja transferências de dados entre Regiões da AWS
- Conceder acesso a atributos específicos do Amazon DynamoDB
- Restringir as alterações nas configurações da VPC
- Exigir atestado para usar uma chave AWS KMS

Exigir acesso de endereços IP específicos

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Esta política permite que o usuário `john_stiles` assuma perfis do IAM somente se a chamada for proveniente de um endereço IP nos intervalos `192.0.2.0/24` ou `203.0.113.0/24`. Essa

política pode ajudar a evitar a divulgação não intencional de dados pessoais e transferências transfronteiriças indesejadas de dados. Por exemplo, se sua organização tem uma equipe de suporte ao cliente que exige acesso a dados pessoais, talvez você queira que essa equipe de suporte acesse esses dados somente de escritórios localizados em um subconjunto específico Regiões da AWS. Além disso, verifique a definição de PII da sua organização, pois algumas políticas podem exigir as seções `Condition` ou `Principal` que restringem o acesso a um usuário ou endereço IP específico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

Exigir associação à organização para acessar os recursos da VPC

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Essa política de VPC endpoint permite que somente diretores e recursos AWS Identity and Access Management (IAM) da `o-1abcde123` organização acessem endpoints Amazon Personalize (Amazon S3). Esse controle preventivo ajuda a estabelecer uma zona de confiança e a definir o perímetro de dados pessoais. Para obter mais informações sobre como essa política pode ajudar a proteger a privacidade e os dados pessoais em sua organização, consulte AWS PrivateLink neste guia.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

Restrinja transferências de dados entre Regiões da AWS

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Com exceção de duas funções AWS Identity and Access Management (IAM), essa política de controle de serviço nega chamadas de API para Serviços da AWS regiões que não Regiões da AWS sejam `eu-west-1` e. `eu-central-1` Esse SCP pode ajudar a impedir a criação de serviços de AWS armazenamento e processamento em regiões não aprovadas. Isso pode ajudar a evitar que dados pessoais sejam totalmente manipulados Serviços da AWS nessas regiões. Essa política usa um `NotAction` parâmetro porque considera serviços globais Serviços da AWS, como IAM, e serviços que se integram a serviços globais, como AWS Key Management Service (AWS KMS) e Amazon CloudFront. Nos valores dos parâmetros, você pode especificar esses serviços globais e outros serviços não aplicáveis como exceções. Para obter mais informações sobre como essa política pode ajudar a proteger a privacidade e os dados pessoais em sua organização, consulte AWS Organizations neste guia.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
```

```
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
```

```
        }
    ]
}
```

Conceder acesso a atributos específicos do Amazon DynamoDB

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

À medida que sua organização discute estratégias para separar física e logicamente os dados pessoais, considere quais serviços de AWS armazenamento oferecem suporte a políticas de controle de acesso refinadas no (IAM). AWS Identity and Access Management A política baseada em identidade a seguir permite a recuperação somente dos atributos `UserID`, `SignUpTime` e `LastLoggedIn` e de uma tabela do Amazon DynamoDB denominada `Users`. Por exemplo, você pode anexar essa política a um perfil de suporte ao cliente em vez de dar a esse perfil acesso ao conjunto de dados pessoais completo. Para obter mais informações sobre como essa política pode ajudar a proteger a privacidade e os dados pessoais em sua organização, consulte Serviços da AWS e recursos que ajudam a segmentar dados neste guia.

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
```

```
                "SignUpTime",
                "LastLoggedIn"
            ]
         },
         "StringEquals":{
            "dynamodb:Select":[
               "SPECIFIC_ATTRIBUTES"
            ]
         }
      }
   ]
}
```

Restringir as alterações nas configurações da VPC

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Depois de projetar e implantar a AWS infraestrutura que suporta seus requisitos de transferência de dados transfronteiriça, que inclui fluxos de dados de rede, talvez você queira evitar modificações. A política de controle de serviço a seguir ajuda a evitar desvios na configuração da VPC ou modificações não intencionais. Ela nega novos anexos de gateway da internet, conexões de emparelhamento da VPC, anexos do gateway de trânsito e novas conexões da VPN. Para obter mais informações sobre como essa política pode ajudar a proteger a privacidade e os dados pessoais em sua organização, consulte AWS Transit Gateway neste guia.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
```

```
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Exigir atestado para usar uma chave AWS KMS

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

A política de chaves a seguir AWS Key Management Service (AWS KMS) permite que as instâncias do AWS Nitro Enclave usem uma chave KMS somente se o documento de atestado do enclave na solicitação corresponder às medidas na declaração de condição. Esta política permite que somente enclaves confiáveis descriptografem os dados. Para obter mais informações sobre como essa política pode ajudar a proteger a privacidade e os dados pessoais em sua organização, consulte AWS Enclaves Nitro neste guia. Para obter uma lista completa das chaves de AWS KMS

condição que podem ser usadas nas políticas de chaves e nas políticas AWS Identity and Access Management (IAM), consulte Chaves de condição para AWS KMS.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
               "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
               "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
               "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
               "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

Elaboração de estratégias para uma expansão global

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

AWS Os Serviços de Garantia de Segurança frequentemente recebem perguntas sobre a arquitetura de privacidade durante a expansão global. AWS As perguntas giram em torno de preocupações com a manutenção da conformidade com requisitos de privacidade exclusivos, como obrigações de soberania de dados ou contratos com clientes, evitando custos adicionais e sobrecarga operacional. As considerações de design geralmente incluem residência de dados, restrição de acesso do operador, resiliência e capacidade de sobrevivência e independência geral. Para obter mais informações, consulte Atendendo aos requisitos de soberania digital em AWS (apresentação do AWS re:Invent 2022).

As seguintes perguntas são comuns e somente você pode respondê-las para seu caso de uso:

- Onde os dados pessoais dos meus clientes precisam residir?
- Onde os dados dos meus clientes estão armazenados?
- Como e onde os dados pessoais podem cruzar fronteiras?
- O acesso humano ou de serviços aos dados entre regiões constitui uma transferência?
- Como posso ter certeza de que nenhum governo estrangeiro vai acessar os dados pessoais dos meus clientes?
- Onde posso armazenar meus backups e locais quentes e frios?
- Para manter os dados locais, devo manter um AWS landing zone em todas as regiões em que presto serviços? Ou posso usar uma AWS Control Tower landing zone existente?

Para requisitos de residência de dados, diferentes implantações de arquitetura podem funcionar melhor para diferentes organizações. Algumas organizações podem exigir que os dados pessoais de seus clientes permaneçam em uma região específica. Nesse caso, você pode ficar preocupado em como cumprir os regulamentos em geral e, ao mesmo tempo, cumprir essas obrigações. Independentemente da situação, há várias considerações ao escolher uma estratégia de implantação de várias contas.

Para definir os principais componentes do projeto de arquitetura, trabalhe em estreita colaboração com suas equipes de conformidade e contrato para confirmar os requisitos de onde, quando e como os dados pessoais podem cruzar as Regiões da AWS. Determine o que se qualifica como uma transferência de dados, como mover, copiar ou visualizar. Além disso, entenda se há controles específicos de resiliência e proteção de dados que devem ser implementados. As estratégias de backup e recuperação de desastres exigem failover entre regiões? Nesse caso, determine quais regiões você pode usar para armazenar seus dados de backup. Determine se há algum requisito para criptografia de dados, como um algoritmo de criptografia específico ou módulos de segurança de hardware dedicados para a geração de chaves. Depois de se alinhar com as partes interessadas em conformidade sobre esses tópicos, comece a considerar abordagens de projeto para seu ambiente de várias contas.

Confira três abordagens que você pode usar para planejar sua estratégia de várias contas da AWS , em ordem crescente de segregação da infraestrutura:

- Zona de pouso central com regiões gerenciadas
- Zonas de pouso regionais
- AWS Nuvem soberana europeia

Também é importante lembrar que a conformidade com a privacidade pode não se limitar apenas à soberania de dados. Leia o restante deste guia para entender as possíveis soluções para muitos outros desafios, como gerenciamento de consentimento, solicitações de titulares de dados, governança de dados e viés de IA.

Zona de pouso central com regiões gerenciadas

Se você deseja expandir globalmente, mas já estabeleceu uma arquitetura de várias contas AWS, é comum usar a mesma landing zone de várias contas (MALZ) para gerenciar outras. Regiões da AWS Nessa configuração, você continuaria operando serviços de infraestrutura, como registro, fábrica de contas e administração geral, a partir de sua AWS Control Tower landing zone existente, na região em que você a criou.

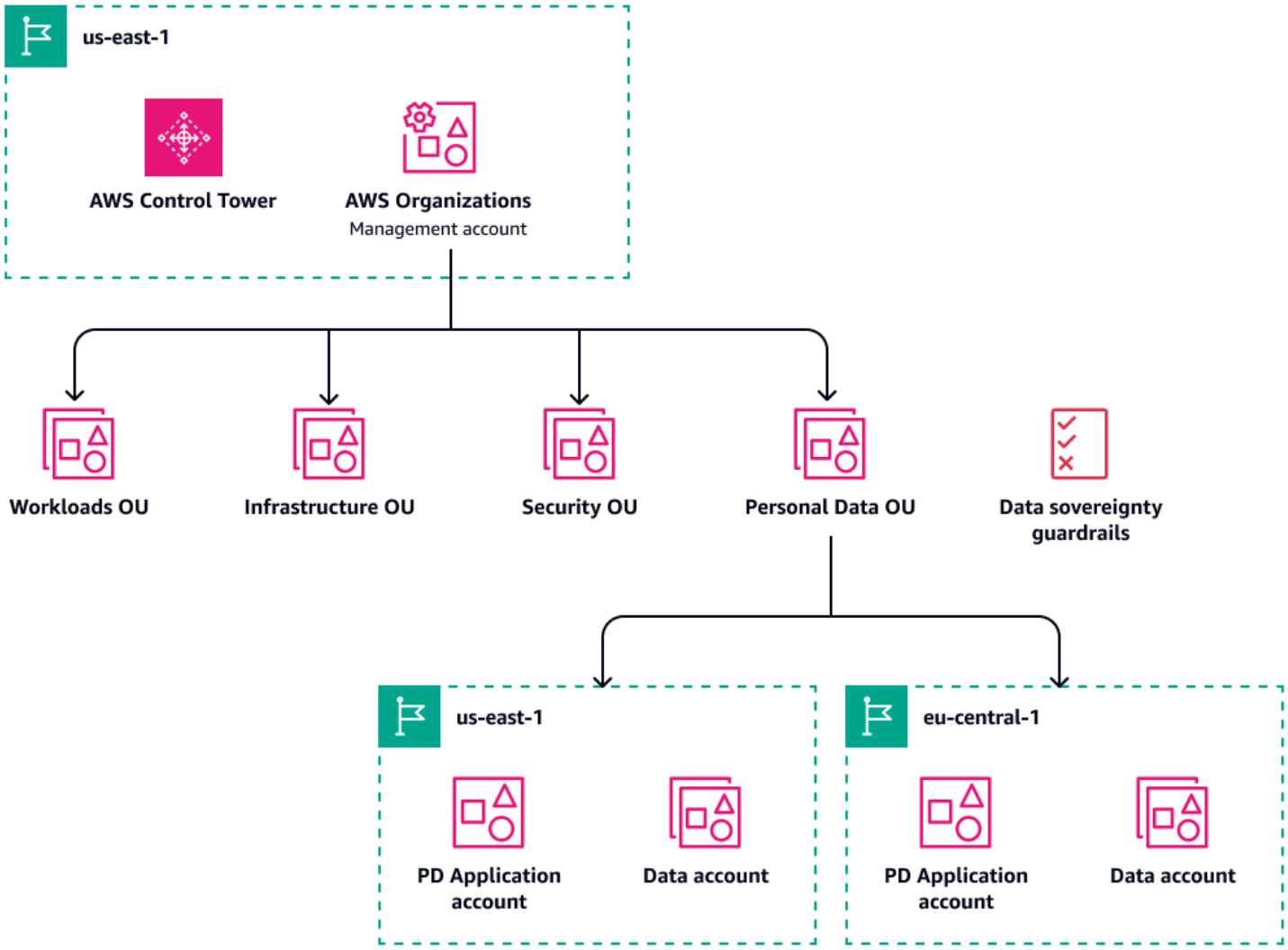
Para workloads de produção, você pode operar implantações regionais estendendo a zona de pouso do AWS Control Tower para uma nova região. Ao fazer isso, você pode estender a governança do AWS Control Tower para a nova região. Dessa forma, você pode manter os armazenamentos de dados pessoais em uma região gerenciada específica. Os dados ainda residem em contas que se beneficiam dos serviços de infraestrutura e da AWS Control Tower governança. Em AWS

Organizations, as contas que contêm dados pessoais ainda se acumulam em uma OU de dados pessoais dedicada, na qual todas as barreiras de soberania de dados são implementadas. AWS Control Tower Além disso, as workloads específicas da região estão contidas em contas dedicadas, em vez de estabelecer contas de produção que podem conter a mesma workload em várias regiões.

Essa implantação pode ser a mais econômica, mas é necessária uma consideração adicional para controlar o fluxo de dados pessoais entre Conta da AWS fronteiras regionais. Considere o seguinte:

- Os logs podem conter dados pessoais, portanto, algumas configurações adicionais podem ser necessárias para conter ou ocultar campos sensíveis para evitar a transferência entre regiões durante a agregação. Para obter mais informações e as práticas recomendadas para controlar a agregação de logs entre regiões, consulte Armazenamento de log centralizado neste guia.
- Considere o isolamento VPCs e o fluxo de tráfego de rede bidirecional apropriado no AWS Transit Gateway design. Você pode limitar quais anexos do gateway de trânsito são permitidos e aprovados, além de limitar quem ou o que pode alterar as tabelas de rotas da VPC.
- Talvez seja necessário impedir que membros da sua equipe de operações de nuvem acessem dados pessoais. Por exemplo, logs de aplicações que contêm dados de transações de clientes podem ser considerados de maior sensibilidade do que outras fontes de logs. Aprovações adicionais e barreiras de proteção técnicas podem ser necessárias, como controle de acesso baseado em perfil e controle de acesso baseado em atributo. Além disso, os dados podem estar sujeitos a limitações de residência quando se trata de acesso. Por exemplo, dados em uma região A só podem ser acessados de dentro dessa região.

O diagrama a seguir mostra uma zona de pouso centralizada com implantações regionais.



Zonas de pouso regionais

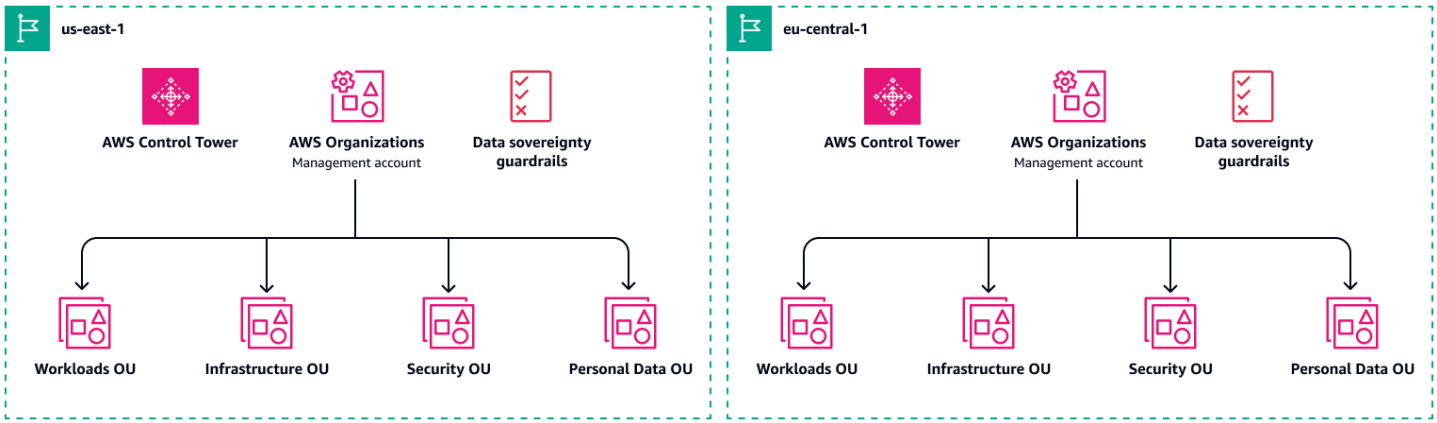
Ter mais de um MALZ pode ajudá-lo a atingir requisitos de conformidade mais rígidos, isolando completamente as cargas de trabalho que processam dados pessoais em comparação com as cargas de trabalho não materiais. AWS Control Tower a agregação centralizada de registros pode ser configurada por padrão e, portanto, simplificada. Com essa abordagem, você não precisa manter exceções para registro em log com fluxos separados de logs que exigem ocultação. Você pode até mesmo ter uma equipe de operações de nuvem local e dedicada para cada MALZ, o que limita o acesso do operador à residência local.

Muitas organizações têm implantações separadas de zona de pouso baseadas nos EUA e na UE. Cada zona de pouso regional tem uma postura de segurança única e abrangente e governança associada para contas na região. Por exemplo, a criptografia de dados pessoais usando dados

dedicados HSMs pode não ser necessária em cargas de trabalho em um MALZ, mas pode ser necessária em outro MALZ.

Embora essa estratégia possa ser dimensionada para atender a muitos requisitos atuais e futuros, é importante compreender os custos adicionais e a sobrecarga operacional associados à manutenção de vários MALZs. Para obter mais informações, consulte Preços do AWS Control Tower.

O diagrama a seguir mostra zonas de pouso separadas em duas regiões.



AWS Nuvem soberana europeia

Algumas organizações exigem uma separação completa de suas workloads que operam no Espaço Econômico Europeu (EEE) e workloads que operam em outros lugares. Nessa situação, considere a nuvem soberana europeia da AWS. A nuvem soberana europeia da AWS é uma nuvem nova e independente para a Europa, projetada para ajudar os clientes a atender às crescentes necessidades de soberania da região, incluindo requisitos rigorosos de residência de dados, autonomia operacional e resiliência.

A AWS European Sovereign Cloud é física e logicamente separada da existente Regiões da AWS, oferecendo a mesma segurança, disponibilidade e desempenho. Somente AWS funcionários localizados na UE têm controle das operações e do suporte da Nuvem Soberana AWS Europeia. Se você tiver requisitos rigorosos de residência de dados, a AWS European Sovereign Cloud mantém todos os metadados que você cria (como as funções, permissões, rótulos de recursos e configurações que eles usam para executar) na UE. AWS A AWS European Sovereign Cloud também possui seus próprios sistemas de medição de faturamento e uso.

Para essa abordagem, você usará um padrão semelhante ao da seção anterior, Zonas de pouso regionais. No entanto, para os serviços que você fornece aos clientes europeus, você pode implantar um MALZ dedicado na AWS European Sovereign Cloud.

Recursos

> **Pesquisa**
>
> Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Recomendações da AWS

- AWS Security Reference Architecture (AWS SRA)

AWSDocumentação da

- Proteção de dados (AWS Well-Architected Framework)
- Data classification (whitepaper da AWS)
- Amazon Web Services: Risk and Compliance (whitepaper da AWS)
- Hybrid architectures to address personal data processing requirements (whitepaper da AWS)
- Navigating GDPR Compliance on AWS (whitepaper da AWS)
- Building a data perimeter on AWS (whitepaper da AWS)
- Documentação de segurança da AWS

Outros recursos da AWS

- Programas de conformidade da AWS
- AWS Modelo de responsabilidade compartilhada da
- Perguntas frequentes sobre privacidade de dados
- AWS Security Assurance Services
- AWS Digital Sovereignty Pledge: Control without compromise (publicação do Blog da AWS)
- AWS Security Learning

Colaboradores

Pesquisa

Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

Este guia foi criado pela equipe do AWS Security Assurance Services. Para obter suporte na implementação das recomendações deste guia e na operacionalização de suas workloads, entre em contato com a equipe do AWS Security Assurance Services.

Autores principais

- Amber Welch, consultora sênior de privacidade da AWS
- Daniel Nieters, consultor principal de privacidade da AWS
- Robert Carter, gerente de programa técnico da AWS

Colaboradores

- Avik Mukherjee, consultor sênior de segurança da AWS
- David Bounds, arquiteto sênior de soluções da AWS
- Jeff Lombardo, arquiteto sênior de soluções de segurança da AWS
- Ram Ramani, arquiteto principal de soluções de segurança da AWS
- Vanessa Jacobs, consultora sênior de segurança da AWS
- Thomas Nicholson, consultor sênior de privacidade da AWS
- Jose DeJesus, consultor sênior de garantia da AWS
- Doug Pardue, gerente de arquitetura de soluções da AWS

Escritores técnicos

- Lilly AbouHarb, redatora técnica sênior da AWS

Histórico do documento

Pesquisa

Gostaríamos muito de ouvir você. Forneça feedback sobre o AWS PRA respondendo a uma breve pesquisa.

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

Alteração	Descrição	Data
Atualizações significativas	Foi adicionado o Catálogo de Controles de Conformidade para Computação em Nuvem (C5) à seção do AWS Artifact. Foi adicionado o Amazon Security Lake à conta do Log Archive. Foram adicionados o Amazon Bedrock, o AWS Clean Rooms, o Amazon DataZone, o AWS Lake Formation, o Amazon SageMaker AI e os recursos e Serviços da AWS que ajudam a descobrir, classificar ou catalogar dados na conta do PD Application. Foi adicionada a seção Estratégias para expansão global.	16 de setembro de 2025
Atualizações significativas	Fizemos atualizações significativas de ponta a ponta.	26 de março de 2024
Publicação inicial	—	2 de outubro de 2023

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributo.

serviços abstraídos

Veja serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

AGGREGATE FUNCTION

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

AI

Veja inteligência artificial.

AIOps

Veja operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicações

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Zona de disponibilidade

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

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

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

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

B

bot malicioso

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

BCP

Veja planejamento de continuidade de negócios

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

Acesso de emergência

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

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

planejamento de continuidade de negócios (BCP)

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

C

CAF

Veja AWS Cloud Adoption Framework.

implantação canário

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

CCoE

Veja Centro de Excelência da Nuvem.

CDC

Veja captura de dados de alteração.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja integração e entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

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

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

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

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

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

CMDB

Veja banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

desvio de dados

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

dados em trânsito

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

data mesh

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Veja linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

implantação

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

ambiente de desenvolvimento

Veja ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja recuperação de desastres.

Detecção da oscilação

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

DVSM

Veja mapeamento do fluxo de valor de desenvolvimento.

E

EDA

Veja análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja endpoint de serviço.

serviço de endpoint

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

planejamento de recursos empresariais (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja planejamento de recursos empresariais.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

Antecipar-se à falha

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

delimitação de isolamento contra falhas

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

ramificação de recursos

Veja ramificação.

recursos

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

importância do recurso

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

transformação de recursos

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

prompt few shot

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

FGAC

Veja controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja modelo de base.

modelo de base (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

golden image

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

estratégia greenfield

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

barreira de proteção

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

H

HA

Veja alta disponibilidade.

migração heterogênea de bancos de dados

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

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

alta disponibilidade (HA)

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

modernização de historiador

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

dados de hold-out

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

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

eu

IaC

Veja infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja Internet das Coisas Industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das coisas (IoT)

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

interpretabilidade

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

IoT

Veja Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Veja biblioteca de informações de TI.

ITSM

Veja gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

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

grande modelo de linguagem (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulo.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

LLM

Veja grande modelo de linguagem.

ambientes inferiores

Veja ambiente.

M

machine learning (ML)

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

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

ramificação principal

Veja ramificação.

Malware

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

Serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Veja Programa de Aceleração da Migração.

mecanismo

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

conta de membro

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

MES

Veja sistema de execução de manufatura.

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

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

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

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja machine learning.

modernização

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

avaliação de preparação para modernização

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

aplicações monolíticas (monólitos)

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

MPA

Veja Avaliação do Portfólio para Migração.

MQTT

Veja Transporte de Telemetria de Enfileiramento de Mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja controle de acesso de origem.

OAI

Veja identidade de acesso de origem.

OCM

Veja gerenciamento de alterações organizacionais.

migração offline

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

OI

Veja integração de operações.

Ola

Veja acordo de nível operacional.

migração online

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

OPC-UA

Veja Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (TO)

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

ORR

Veja análise de prontidão operacional.

OT

Veja tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja informações de identificação pessoal.

manual

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

PLC

Veja controlador lógico programável.

PLM

Veja gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pushdown de predicados

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

controle preventivo

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

principal (entidade principal)

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

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja ambiente.

controlador lógico programável (PLC)

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

encadeamento de prompts

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

pseudonimização

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

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

RAG

Veja geração aumentada via recuperação.

ransomware

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

Matriz RASCI

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

RCAC

Veja controle de acesso por linha e coluna.

réplica de leitura

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

Redefinir arquitetura

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

Retirada

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja objetivo de ponto de recuperação.

RTO

Veja objetivo de tempo de recuperação.

runbook

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

S

SAML 2.0

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja política de controle de serviço.

secret

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

segurança desde a concepção

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

controle de segurança

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

hardening da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja sistema de gerenciamento de eventos e informações de segurança.

ponto único de falha (SPOF)

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

SLA

Veja cacordo de serviço.

SLI

Veja indicador de nível de serviço.

SLO

Veja objetivo de nível de serviço.

split-and-seed modelo

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

SPOF

Veja ponto único de falha.

esquema em estrela

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

padrão strangler fig

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

sub-rede

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

controle supervisório e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

WORM

Veja gravação única e várias leituras.

WQF

Veja AWS Workload Qualification Framework.

gravação única e várias leituras (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

prompt zero shot

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

eficácia dos prompts zero-shot depende da complexidade da tarefa e da qualidade do prompt. Veja também prompts few-shot.

aplicação zumbi

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

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