AWS Arquitetura de referência de segurança (AWS SRA) — arquitetura principal

AWS Orientação prescritiva

AWS Orientação prescritiva: AWS Arquitetura de referência de segurança (AWS SRA) — arquitetura principal

Table of Contents

AWS Arquitetura de referência de segurança (AWS SRA) — arquitetura principal

Equipe de segurança de serviços globais, Amazon Web Services (colaboradores)

Dezembro de 2025 (histórico do documento)

> Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

A Arquitetura de Referência de Segurança (AWS SRA AWS) da Amazon Web Services () é um conjunto holístico de diretrizes para implantar o conjunto completo de serviços de AWS segurança em um ambiente com várias contas. Use-o para ajudar a projetar, implementar e gerenciar serviços AWS de segurança para que eles se alinhem às práticas AWS recomendadas. As recomendações são criadas com base em uma arquitetura de página única que inclui serviços de AWS segurança — como eles ajudam a atingir os objetivos de segurança, onde eles podem ser melhor implantados e gerenciados e como eles interagem com outros serviços de segurança. Contas da AWS Essa orientação geral de arquitetura complementa as recomendações detalhadas e específicas do serviço, como as encontradas no site da Documentação de AWS Segurança.

A arquitetura e as recomendações que a acompanham são baseadas em nossas experiências coletivas com clientes AWS corporativos. Este documento é uma referência — um conjunto abrangente de diretrizes Serviços da AWS para uso na proteção de um ambiente específico — e os padrões de solução no repositório de códigos da AWS SRA foram projetados para a arquitetura específica ilustrada nesta referência. Cada cliente terá requisitos diferentes. Como resultado, o design do seu AWS ambiente pode ser diferente dos exemplos fornecidos aqui. Você precisará modificar e adaptar essas recomendações para atender às suas necessidades individuais de ambiente e segurança. Em todo o documento, quando apropriado, sugerimos opções para cenários alternativos vistos com frequência.

O AWS SRA é um conjunto dinâmico de orientações e é atualizado periodicamente com base nos novos lançamentos de serviços e recursos, no feedback dos clientes e no cenário de ameaças em constante mudança. Cada atualização incluirá a data da revisão e o registro de alterações associado.

Embora confiemos em um diagrama de uma página como base, a arquitetura é mais profunda do que um único diagrama de blocos e deve ser construída sobre uma base bem estruturada de fundamentos e princípios de segurança. Você pode usar esse documento de duas maneiras: como narrativa ou como referência. Os tópicos são organizados como uma história, para que você possa lê-los do início (orientação básica de segurança) até o fim (discussão de exemplos de código que você pode implementar). Como alternativa, você pode navegar pelo documento para se concentrar nos princípios de segurança, nos serviços, nos tipos de conta, nas orientações e nos exemplos mais relevantes às suas necessidades.

Este documento está dividido nas seguintes seções e em um apêndice:

- Sobre a biblioteca da AWS SRA fornece uma visão geral da orientação técnica e do código incluídos na coleção de AWS publicações da SRA.
- O valor do AWS SRA discute a motivação para criar o AWS SRA, descreve como você pode usá-lo para ajudar a melhorar sua segurança e lista as principais conclusões.
- As fundações de segurança revisam o AWS Cloud Adoption Framework (AWS CAF), o AWS Well-Architected Framework e AWS o Shared Responsibility Model, destacando elementos que são especialmente relevantes para o SRA. AWS
- AWS Organizations, accounts and IAM guardrails apresenta o AWS Organizations serviço, discute os recursos básicos de segurança e as barreiras de proteção e fornece uma visão geral de nossa estratégia recomendada para várias contas.
- A Arquitetura de Referência de AWS Segurança é um diagrama de arquitetura de página única que mostra a funcionalidade Contas da AWS e os serviços e recursos de segurança que estão geralmente disponíveis.
- A IA/ML para segurança descreve como os diferentes Serviços da AWS usam inteligência artificial e aprendizado de máquina (AI/ML) em segundo plano para ajudar você a atingir objetivos de segurança específicos. Você pode incluí-los Serviços da AWS em seu design para aproveitar os recursos avançados de segurança.
- Construindo sua arquitetura de segurança – Uma abordagem em fases fornece orientação sobre como você pode criar sua própria arquitetura de segurança em seis fases iterativas, com base na referência fornecida pela AWS SRA.
- AWS A lista de verificação de melhores práticas da SRA resume as recomendações discutidas ao longo do guia em uma lista de verificação que você pode seguir ao criar sua versão da arquitetura de segurança.

- Os recursos do IAM apresentam um resumo e um conjunto de dicas para orientação AWS Identity and Access Management (IAM) que são importantes para sua arquitetura de segurança.
- O repositório de código para exemplos de AWS SRA fornece uma visão geral do GitHub repositório associado que ajudará desenvolvedores e engenheiros a implantar alguns dos padrões de orientação e arquitetura apresentados neste documento. Você pode implantar as amostras usando AWS CloudFormation ou o Terraform by HashiCorp. Eles oferecem suporte a AWS Control Tower ambientes AWS Control Tower tanto quanto não.

O apêndice contém uma lista dos serviços individuais de AWS segurança, identidade e conformidade e fornece links para mais informações sobre cada serviço. A seção Histórico do documento fornece um registro de alterações para rastrear versões deste documento. Você também pode assinar um feed RSS para receber notificações de alterações.

Sobre a biblioteca AWS SRA

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Este guia faz parte de uma biblioteca que fornece planos arquitetônicos e orientação técnica para projetar e criar arquiteturas de segurança em. AWS A biblioteca consiste em código de implementação (biblioteca de códigos AWS SRA), uma ferramenta de validação (SRA Verify) e duas categorias complementares de guias que abrangem a arquitetura principal e as arquiteturas de aprofundamento.

AWS SRA — arquitetura principal (este guia)

Este guia representa a base para a arquitetura AWS de segurança recomendada. É o ponto de partida que se aplica a todas as organizações, independentemente do setor, do tipo de aplicativo ou de qualquer outra consideração. Essa base ajuda você a criar uma arquitetura forte e escalável AWS e ajuda a criar uma linha de base sólida de segurança para AWS várias contas que se expande com segurança à medida que sua empresa cresce.

AWS SRA — arquiteturas de mergulho profundo

O AWS SRA — guia de arquitetura principal é complementado por publicações adicionais que fornecem padrões de arquitetura alinhados a recursos específicos de segurança, tipos de aplicativos e requisitos regulatórios ou de conformidade. Esses padrões estendem a arquitetura principal e devem ser usados em conjunto com o AWS SRA — guia de arquitetura central.

Os guias a seguir fornecem padrões de arquitetura alinhados a recursos de segurança específicos:

- AWS SRA — gerenciamento de identidade fornece orientação sobre como implementar uma solução de gerenciamento de identidade e acesso escalável, robusta e centralizada no. AWS
- AWS SRA — a segurança perimetral discute os padrões de arquitetura e Serviços da AWS a implementação da segurança de ponta em uma conta central ou em contas individuais.
- AWS SRA — análise forense cibernética descreve como configurar uma conta AWS forense como ponto de partida para desenvolver as capacidades forenses de sua organização e ajudar a melhorar sua preparação para a resposta a incidentes de segurança (IR).

Os guias a seguir fornecem padrões de arquitetura para tipos específicos de aplicativos. Talvez você queira se concentrar neles depois de criar sua arquitetura de segurança básica:

- AWS SRA — A segurança de IA fornece recomendações de arquitetura de segurança para projetar e criar aplicativos que incorporem recursos de IA generativa usando serviços de IA AWS generativa.
- AWS SRA — IoT fornece recomendações de arquitetura de segurança para projetar e criar aplicativos de IoT em. AWS

Além disso, o guia a seguir descreve padrões de arquitetura que estão alinhados com estruturas regulatórias ou de conformidade específicas:

- AWS A Privacy Reference Architecture (AWS PRA) fornece uma arquitetura de segurança para aplicativos que processam dados pessoais e deve suportar amplos requisitos de conformidade de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Privacidade do Consumidor da Califórnia (CCPA) ou a Lei Geral de Proteção de Dados do Brasil (LGPD). O AWS PRA fornece um conjunto de diretrizes específicas para o design e configuração dos controles de privacidade em Serviços da AWS.

Recomendamos que você comece com o AWS SRA — guia de arquitetura principal para entender a arquitetura fundamental e, em seguida, consulte os guias complementares para aproveitar as funcionalidades e implementações avançadas. Para obter mais informações sobre esse conjunto de conteúdo, consulte Arquitetura AWS de referência de segurança.

> **Diagramas de arquitetura**
>
> Para personalizar os diagramas da arquitetura de referência na biblioteca AWS SRA com base nas necessidades de sua empresa, você pode baixar o seguinte arquivo.zip e extrair seu conteúdo.
>
> Baixe o arquivo de origem do diagrama (PowerPointformato Microsoft)

O valor do AWS SRA

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

AWS tem um grande (e crescente) conjunto de serviços de segurança e relacionados à segurança. Os clientes expressaram gratidão pelas informações detalhadas disponíveis por meio de nossa documentação de serviço, postagens em blogs, tutoriais, conferências e conferências. Eles também nos dizem que querem entender melhor o panorama geral e ter uma visão estratégica dos serviços de AWS segurança. Quando trabalhamos com clientes para obter uma apreciação mais profunda do que eles precisam, surgem três prioridades:

- Os clientes querem mais informações e padrões recomendados sobre como eles podem implantar, configurar e operar os serviços de AWS segurança de forma holística. Em quais contas e para quais objetivos de segurança os serviços devem ser implantados e gerenciados? Existe uma conta de segurança na qual todos ou a maioria dos serviços devem operar? Como a escolha do local (unidade organizacional ou Conta da AWS) influencia os objetivos de segurança? Quais compensações (considerações de design) os clientes devem conhecer?
- Os clientes estão interessados em ver perspectivas diferentes para organizar logicamente os diversos serviços AWS de segurança. Além da função principal de cada serviço (por exemplo, serviços de identidade ou serviços de registro), esses pontos de vista alternativos ajudam os clientes a planejar, projetar e implementar sua arquitetura de segurança. Um exemplo compartilhado posteriormente neste documento agrupa os serviços com base nas camadas de proteção alinhadas à estrutura recomendada do seu AWS ambiente.
- Os clientes estão procurando orientação e exemplos para integrar os serviços de segurança da maneira mais eficaz. Por exemplo, como eles devem se alinhar e se conectar melhor AWS Config com outros serviços para fazer o trabalho pesado em pipelines automatizados de auditoria e monitoramento? Os clientes estão pedindo orientação sobre como cada serviço de AWS segurança depende ou oferece suporte a outros serviços de segurança.

Abordamos cada um deles no AWS SRA. A primeira prioridade na lista (para onde as coisas vão) é o foco do diagrama da arquitetura principal e das discussões que o acompanham neste documento. Fornecemos uma AWS Organizations arquitetura recomendada e uma account-by-account descrição de quais serviços vão para onde. Para começar com a segunda prioridade da lista (como pensar no

conjunto completo de serviços de segurança), leia a seção Aplicar serviços de segurança em sua AWS organização. Esta seção descreve uma forma de agrupar os serviços de segurança de acordo com a estrutura dos elementos em sua AWS organização. Além disso, essas mesmas ideias são refletidas na discussão da conta Application, que destaca como os serviços de segurança podem ser operados para se concentrar em determinadas camadas da conta: instâncias do Amazon Elastic Compute Cloud (Amazon EC2), redes Amazon Virtual Private Cloud (Amazon VPC) e a conta mais ampla. Finalmente, a terceira prioridade (integração de serviços) se reflete em toda a orientação, particularmente na discussão de serviços individuais nos guias de aprofundamento na biblioteca da AWS SRA e do código no repositório de códigos da SRA. AWS

Como usar o AWS SRA

Há diferentes maneiras de usar o AWS SRA, dependendo de onde você está em sua jornada de adoção da nuvem. Aqui está uma lista de maneiras de obter o máximo de informações sobre os ativos da AWS SRA (diagrama de arquitetura, orientação escrita e exemplos de código).

- Defina o estado de destino para sua própria arquitetura de segurança.

  Se você está apenas começando sua Nuvem AWS jornada, configurando seu primeiro conjunto de contas, ou planejando aprimorar um AWS ambiente estabelecido, o AWS SRA é o lugar para começar a criar sua arquitetura de segurança. Comece com uma base abrangente de estrutura de contas e serviços de segurança e, em seguida, ajuste com base em sua pilha de tecnologia, habilidades, objetivos de segurança e requisitos de conformidade específicos. Se você sabe que criará e lançará mais cargas de trabalho, pode usar sua versão personalizada do AWS SRA como base para a arquitetura de referência de segurança da sua organização. Para descobrir como você pode atingir o estado alvo descrito pela AWS SRA, consulte a seção Construindo sua arquitetura de segurança — Uma abordagem em fases.
- Revise (e revise) os projetos e os recursos que você já implementou.

  Se você já tem um projeto e uma implementação de segurança, vale a pena dedicar algum tempo para comparar o que você tem com o AWS SRA. O AWS SRA foi projetado para ser abrangente e fornecer uma linha de base de diagnóstico para analisar sua própria segurança. Quando seus projetos de segurança se alinham ao AWS SRA, você pode se sentir mais confiante de que está seguindo as melhores práticas ao usar. Serviços da AWS Se seus projetos de segurança divergirem ou até discordarem das orientações do AWS SRA, isso não é necessariamente um sinal de que você está fazendo algo errado. Em vez disso, essa observação oferece a oportunidade de revisar seu processo de decisão. Há motivos comerciais e tecnológicos legítimos

pelos quais você pode se desviar das melhores práticas da AWS SRA. Talvez seus requisitos específicos de conformidade, regulamentação ou segurança organizacional exijam configurações de serviço específicas. Ou, em vez de usar Serviços da AWS, você pode ter uma preferência de recurso por um produto do AWS Partner Network ou por um aplicativo personalizado que você criou e gerencia. Às vezes, durante essa análise, você pode descobrir que suas decisões anteriores foram tomadas com base em tecnologias, AWS recursos ou restrições comerciais mais antigas que não se aplicam mais. Essa é uma boa oportunidade para revisar, priorizar todas as atualizações e adicioná-las ao local apropriado da sua lista de pendências de engenharia. O que quer que você descubra ao avaliar sua arquitetura de segurança à luz da AWS SRA, você achará importante documentar essa análise. Ter esse registro histórico das decisões e suas justificativas pode ajudar a informar e priorizar decisões futuras.

- Inicialize a implementação de sua própria arquitetura de segurança.

  Os módulos de infraestrutura como código (IaC) da AWS SRA fornecem uma maneira rápida e confiável de começar a criar e implementar sua arquitetura de segurança. Esses módulos são descritos mais detalhadamente na seção de repositório de código e no GitHub repositório público. Eles não apenas permitem que os engenheiros desenvolvam exemplos de alta qualidade dos padrões na orientação da AWS SRA, mas também incorporam controles de segurança recomendados, como políticas de senha do IAM, acesso público à conta de bloqueio do Amazon Simple Storage Service (Amazon S3), criptografia padrão EC2 da Amazon Elastic Block Store (Amazon EBS) e integração AWS Control Tower para que os controles sejam aplicados ou removidos à medida que novos são integrados ou desativado. Contas da AWS

- Saiba mais sobre serviços e recursos de AWS segurança.

  As orientações e discussões na AWS SRA incluem recursos importantes, bem como considerações de implantação e gerenciamento para AWS segurança individual e serviços relacionados à segurança. Um recurso do AWS SRA é que ele fornece uma introdução de alto nível à amplitude dos serviços de AWS segurança e à forma como eles funcionam juntos em um ambiente com várias contas. Isso complementa o aprofundamento nos recursos e na configuração de cada serviço encontrado em outras fontes. Um exemplo disso é a discussão sobre como o AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) ingere descobertas de segurança de uma variedade de Serviços da AWS AWS Partner produtos e até mesmo de seus próprios aplicativos.

- Promova uma discussão sobre governança organizacional e responsabilidades pela segurança.

Um elemento importante para projetar e implementar qualquer arquitetura ou estratégia de segurança é entender quem em sua organização tem quais responsabilidades relacionadas à segurança. Por exemplo, a questão de onde agregar e monitorar as descobertas de segurança está ligada à questão de qual equipe será responsável por essa atividade. Todas as descobertas em toda a organização são monitoradas por uma equipe central que precisa acessar uma conta dedicada do Security Tooling? Ou as equipes individuais de aplicativos (ou unidades de negócios) são responsáveis por determinadas atividades de monitoramento e, portanto, precisam acessar determinadas ferramentas de alerta e monitoramento? Como outro exemplo, se sua organização tiver um grupo que gerencia todas as chaves de criptografia centralmente, isso influenciará quem tem permissão para criar chaves AWS Key Management Service (AWS KMS) e em quais contas essas chaves serão gerenciadas. Compreender as características de sua organização, as várias equipes e responsabilidades, ajudará você a adaptar o SRA para melhor atender às suas necessidades. AWS Por outro lado, às vezes, a discussão sobre a arquitetura de segurança se torna o ímpeto para discutir as responsabilidades organizacionais existentes e considerar possíveis mudanças. AWS recomenda um processo de tomada de decisão descentralizado em que as equipes de carga de trabalho sejam responsáveis por definir os controles de segurança com base em suas funções e requisitos de carga de trabalho. O objetivo da equipe centralizada de segurança e governança é criar um sistema que permita que os proprietários da carga de trabalho tomem decisões informadas e que todas as partes tenham visibilidade da configuração, das descobertas e dos eventos. O AWS SRA pode ser um veículo para identificar e informar essas discussões.

Principais diretrizes de implementação da AWS SRA

Aqui estão oito principais conclusões do AWS SRA que você deve ter em mente ao projetar e implementar sua segurança.

- AWS Organizations e uma estratégia adequada de várias contas são elementos necessários de sua arquitetura de segurança. A separação adequada de cargas de trabalho, equipes e funções fornece a base para a separação de tarefas e defense-in-depth estratégias. O guia abordará isso mais detalhadamente em uma seção posterior.
- Defense-in-depth é uma consideração de design importante para selecionar controles de segurança para sua organização. Ele ajuda você a injetar os controles de segurança apropriados em diferentes camadas da AWS Organizations estrutura, o que ajuda a minimizar o impacto de um problema: se houver um problema com uma camada, existem controles em vigor que isolam

outros recursos de TI valiosos. O AWS SRA demonstra como diferentes Serviços da AWS funções em diferentes camadas da pilha de AWS tecnologia e como o uso combinado desses serviços ajuda você a alcançar seus objetivos. defense-in-depth Esse defense-in-depth conceito AWS é discutido mais detalhadamente em uma seção posterior, com exemplos de design mostrados em Conta do aplicativo.

- Use a ampla variedade de componentes de segurança em vários Serviços da AWS recursos para criar uma infraestrutura de nuvem robusta e resiliente. Ao adaptar o AWS SRA às suas necessidades específicas, considere não apenas a função Serviços da AWS e os recursos principais (por exemplo, autenticação, criptografia, monitoramento, política de permissão), mas também como eles se encaixam na estrutura de sua arquitetura. Uma seção posterior do guia descreve como alguns serviços operam em toda a AWS organização. Outros serviços funcionam melhor em uma única conta, e alguns são projetados para conceder ou negar permissão a diretores individuais. A consideração dessas duas perspectivas ajuda você a criar uma abordagem de segurança mais flexível e em camadas.
- Sempre que possível (conforme detalhado nas seções posteriores), use o Serviços da AWS que pode ser implantado em todas as contas (distribuídas em vez de centralizadas) e crie um conjunto consistente de proteções compartilhadas que possam ajudar a proteger suas cargas de trabalho contra o uso indevido e a reduzir o impacto de eventos de segurança. O AWS SRA usa AWS Security Hub CSPM (monitoramento centralizado de localização e verificações de conformidade), Amazon GuardDuty (detecção de ameaças e detecção de anomalias) AWS Config (monitoramento de recursos e detecção de alterações), IAM Access Analyzer (monitoramento de acesso a recursos), AWS CloudTrail (registro da atividade da API do serviço em seu ambiente) e Amazon Macie (classificação de Serviços da AWS dados) como um conjunto básico a ser implantado em todos os ambientes. Conta da AWS
- Use o recurso de administração delegada do AWS Organizations, onde houver suporte, conforme explicado posteriormente na seção de administração delegada do guia. Isso permite que você registre uma conta de AWS membro como administrador dos serviços suportados. A administração delegada oferece flexibilidade para diferentes equipes de sua empresa usarem contas separadas, conforme apropriado para suas responsabilidades, para gerenciar Serviços da AWS todo o ambiente. Além disso, o uso de um administrador delegado ajuda a limitar o acesso e gerenciar a sobrecarga de permissões da conta de AWS Organizations gerenciamento.
- Implemente monitoramento, gerenciamento e governança centralizados em suas AWS organizações. Ao usar Serviços da AWS essa agregação de suporte de várias contas (e às vezes de várias regiões), junto com recursos de administração delegada, você capacita suas equipes centrais de engenharia de segurança, rede e nuvem a terem ampla visibilidade e controle sobre

a configuração de segurança e a coleta de dados apropriadas. Além disso, os dados podem ser devolvidos às equipes de carga de trabalho para capacitá-las a tomar decisões de segurança eficazes no início do ciclo de vida de desenvolvimento de software (SDLC).

- Use AWS Control Tower para configurar e controlar seu AWS ambiente de várias contas com a implementação de controles de segurança pré-criados para iniciar sua construção de arquitetura de referência de segurança. AWS Control Tower fornece um plano para fornecer gerenciamento de identidade, acesso federado às contas, registro centralizado e fluxos de trabalho definidos para provisionar contas adicionais. Em seguida, você pode usar a solução Customizations for AWS Control Tower (cFCT) para definir as contas gerenciadas AWS Control Tower com controles adicionais de segurança, configurações de serviço e governança, conforme demonstrado pelo repositório de códigos da SRA. AWS O recurso de fábrica de contas provisiona automaticamente novas contas com modelos configuráveis com base na configuração de conta aprovada para padronizar as contas em suas organizações. AWS Você também pode estender a governança a um indivíduo existente Conta da AWS inscrevendo-o em uma unidade organizacional (OU) que já é governada por. AWS Control Tower
- Os exemplos de código do AWS SRA demonstram como você pode automatizar a implementação de padrões no guia do AWS SRA usando a infraestrutura como código (IaC). Ao codificar os padrões, você pode tratar o IaC como outros aplicativos em sua organização e automatizar os testes antes de implantar o código. O IaC também ajuda a garantir a consistência e a repetibilidade implantando grades de proteção em vários ambientes (por exemplo, SDLC ou específicos da região). Os exemplos de código SRA podem ser implantados em um ambiente de AWS Organizations várias contas com ou sem. AWS Control Tower As soluções necessárias neste repositório AWS Control Tower foram implantadas e testadas em um AWS Control Tower ambiente usando AWS CloudFormation e personalizações para AWS Control Tower (cFct). As soluções que não exigem AWS Control Tower foram testadas em um AWS Organizations ambiente usando AWS CloudFormation. Se você não usar AWS Control Tower, poderá usar a solução de implantação AWS Organizations baseada.

Fundamentos de segurança

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O AWS SRA se alinha a três bases de AWS segurança: o AWS Cloud Adoption Framework (AWS CAF), o AWS Well-Architected e o Modelo de Responsabilidade Compartilhada. AWS

AWS A Professional Services criou o AWS CAF para ajudar as empresas a projetar e seguir um caminho acelerado para a adoção bem-sucedida da nuvem. A orientação e as melhores práticas fornecidas pela estrutura ajudam você a criar uma abordagem abrangente para a computação em nuvem em toda a sua empresa e em todo o seu ciclo de vida de TI. O AWS CAF organiza a orientação em seis áreas de enfoque, chamadas perspectivas. Cada perspectiva abrange responsabilidades distintas pertencentes ou gerenciadas por partes interessadas funcionalmente relacionadas. Em geral, as perspectivas de negócios, pessoas e governança têm como foco capacidades de negócios; enquanto as perspectivas de plataforma, segurança e operações concentram-se em capacidades técnicas.

A perspectiva de segurança do AWS CAF ajuda você a estruturar a seleção e a implementação de controles em toda a sua empresa. Seguir as AWS recomendações atuais do pilar de segurança pode ajudá-lo a atender aos requisitos regulamentares e comerciais.

AWS O Well-Architected ajuda os arquitetos de nuvem a criar uma infraestrutura segura, de alto desempenho, resiliente e eficiente para seus aplicativos e cargas de trabalho. A estrutura é baseada em seis pilares — excelência operacional, segurança, confiabilidade, eficiência de desempenho, otimização de custos e sustentabilidade — e fornece uma abordagem consistente para AWS clientes e parceiros avaliarem arquiteturas e implementarem projetos que possam ser expandidos com o tempo. Acreditamos que ter as workloads bem arquitetadas aumenta muito a probabilidade de sucesso nos negócios.

O pilar de segurança do Well-Architected Framework descreve como aproveitar as tecnologias de nuvem para ajudar a proteger dados, sistemas e ativos de uma forma que possa melhorar sua postura de segurança. Isso ajudará você a atender aos requisitos comerciais e regulamentares seguindo as AWS recomendações atuais. Há outras áreas de foco do Well-Architected Framework que fornecem mais contexto para domínios específicos, como governança, sem servidor, IA/ML e jogos. Elas são conhecidas como lentes AWS Well-Architected.

A segurança e a conformidade são uma responsabilidade compartilhada entre o cliente AWS e o cliente. Esse modelo compartilhado pode ajudar a aliviar sua carga operacional, pois AWS opera, gerencia e controla os componentes do sistema operacional host e da camada de virtualização até a segurança física das instalações nas quais o serviço opera. Por exemplo, você assume a responsabilidade e o gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança), do software do aplicativo, da criptografia de dados do lado do servidor, das tabelas de rotas de tráfego de rede e da configuração do firewall do grupo de segurança AWS fornecido. Para serviços abstratos, como Amazon S3 e Amazon DynamoDB AWS , opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. Você é responsável por gerenciar seus dados (incluindo opções de criptografia), classificar seus ativos e usar as ferramentas do IAM para aplicar as permissões apropriadas. Esse modelo compartilhado geralmente é descrito dizendo que AWS é responsável pela segurança da nuvem (ou seja, por proteger a infraestrutura que executa todos os serviços oferecidos na Nuvem AWS) e que você é responsável pela segurança na nuvem (conforme determinado pelos Nuvem AWS serviços selecionados).

Dentro da orientação fornecida por esses documentos fundamentais, dois conjuntos de conceitos são particularmente relevantes para o design e a compreensão do AWS SRA: recursos de segurança e princípios de design de segurança.

Capacidades de segurança

A perspectiva de segurança do AWS CAF descreve nove recursos que ajudam você a alcançar a confidencialidade, integridade e disponibilidade de seus dados e cargas de trabalho na nuvem.

- Governança de segurança para desenvolver e comunicar funções, responsabilidades, políticas, processos e procedimentos de segurança em todo o AWS ambiente da sua organização.
- Garantia de segurança para monitorar, avaliar, gerenciar e melhorar a eficácia de seus programas de segurança e privacidade.
- Gerenciamento de identidade e acesso para gerenciar identidades e permissões em grande escala.
- Detecção de ameaças para entender e identificar possíveis configurações incorretas de segurança, ameaças ou comportamentos inesperados.
- Gerenciamento de vulnerabilidades para identificar, classificar, corrigir e mitigar continuamente as vulnerabilidades de segurança.

- Proteção de infraestrutura para ajudar a validar se os sistemas e serviços em suas cargas de trabalho estão protegidos.
- Proteção de dados para manter a visibilidade e o controle sobre os dados e como eles são acessados e usados em sua organização.
- Segurança de aplicativos para ajudar a detectar e solucionar vulnerabilidades de segurança durante o processo de desenvolvimento de software.
- Resposta a incidentes para reduzir possíveis danos respondendo de forma eficaz aos incidentes de segurança.

Princípios de design de segurança

O pilar de segurança do Well-Architected Framework captura um conjunto de sete princípios de design que transformam áreas de segurança específicas em orientações práticas que podem ajudá-lo a fortalecer a segurança de sua carga de trabalho. Onde os recursos de segurança estruturam a estratégia geral de segurança, esses princípios do Well-Architected Framework descrevem o que você pode começar a fazer. Eles são refletidos de forma muito deliberada neste AWS SRA e consistem no seguinte:

- Implemente uma base sólida de identidade – Implemente o princípio do privilégio mínimo e imponha a separação de tarefas com a autorização apropriada para cada interação com seus AWS recursos. Centralize o gerenciamento de identidades e procure eliminar a dependência de credenciais estáticas de longo prazo.
- Habilite a rastreabilidade – Monitore, gere alertas e audite ações e alterações em seu ambiente em tempo real. Integre a coleta de logs e métricas aos sistemas para investigar e executar ações automaticamente.
- Aplique segurança em todas as camadas – Aplique uma defense-in-depth abordagem com vários controles de segurança. Aplique vários tipos de controles (por exemplo, controles preventivos e de detecção) a todas as camadas, incluindo borda da rede, nuvem privada virtual (VPC), balanceamento de carga, serviços de instância e computação, sistema operacional, configuração de aplicativos e código.
- Automatize as melhores práticas de segurança – Mecanismos de segurança automatizados e baseados em software melhoram sua capacidade de escalar com segurança de forma mais rápida e econômica. Crie arquiteturas seguras e implemente controles definidos e gerenciados como código em modelos com controle de versão.

- Proteja os dados em trânsito e em repouso – Classifique seus dados em níveis de sensibilidade e use mecanismos como criptografia, tokenização e controle de acesso, quando apropriado.
- Mantenha as pessoas afastadas dos dados – Use mecanismos e ferramentas para reduzir ou eliminar a necessidade de acessar diretamente ou processar dados manualmente. Isso reduz o risco de erros de processamento ou modificação e erro humano ao manipular dados confidenciais.
- Prepare-se para eventos de segurança – Prepare-se para um incidente com políticas e processos de gestão e investigação de incidentes alinhados às suas necessidades organizacionais. Execute simulações de resposta a incidentes e use ferramentas com automação para aumentar sua velocidade de identificação, investigação e recuperação.

Como usar o AWS SRA com AWS CAF e Well-Architected Framework AWS

O AWS CAF, o AWS Well-Architected Framework AWS e o SRA são estruturas complementares que trabalham juntas para apoiar seus esforços de migração e modernização para a nuvem.

- O AWS CAF aproveita a AWS experiência e as melhores práticas para ajudá-lo a alinhar os valores da adoção da nuvem aos resultados comerciais desejados. Use o AWS CAF para identificar e priorizar oportunidades de transformação, avaliar e melhorar a prontidão para a nuvem e desenvolver iterativamente seu roteiro de transformação.
- O AWS Well-Architected Framework AWS fornece recomendações para criar uma infraestrutura segura, de alto desempenho, resiliente e eficiente para uma variedade de aplicativos e cargas de trabalho que atendam aos resultados de seus negócios.
- O AWS SRA ajuda você a entender como implantar e governar serviços de segurança de uma forma alinhada às recomendações do AWS CAF e do Well-Architected Framework. AWS

Por exemplo, a perspectiva de segurança do AWS CAF sugere que você avalie como gerenciar centralmente suas identidades de força de trabalho e sua autenticação em. AWS Com base nessas informações, você pode decidir usar uma solução de provedor de identidade corporativa (IdP) nova ou existente, como Okta, Active Directory ou Ping Identity, para essa finalidade. Você segue as orientações do AWS Well-Architected Framework e decide integrar seu IdP ao para oferecer Centro de Identidade do AWS IAM a seus funcionários uma experiência de login único que possa sincronizar suas associações e permissões de grupo. Você analisa a recomendação da AWS SRA para ativar o IAM Identity Center na conta de gerenciamento da sua AWS organização e administrá-lo por meio

de uma conta de ferramentas de segurança usada pela sua equipe de operações de segurança. Este exemplo ilustra como o AWS CAF ajuda você a tomar decisões iniciais sobre a postura de segurança desejada, o AWS Well-Architected Framework fornece a orientação sobre como avaliar o Serviços da AWS que está disponível para atingir esse objetivo e, em seguida, o AWS SRA fornece recomendações sobre como implantar e controlar os serviços de segurança selecionados.

Blocos de construção da SRA — AWS Organizations, contas e grades de proteção

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

AWS os serviços de segurança, seus controles e interações são melhor empregados com base na estratégia de AWS várias contas e nas barreiras de gerenciamento de identidade e acesso. Essas barreiras definem a capacidade de implementação de privilégios mínimos, separação de deveres e privacidade e fornecem suporte para decisões sobre quais tipos de controles são necessários, onde cada serviço de segurança é gerenciado e como eles podem compartilhar dados e permissões na SRA. AWS

E Conta da AWS fornece limites de segurança, acesso e cobrança para seus AWS recursos e permite que você alcance independência e isolamento de recursos. O uso de várias Contas da AWS desempenha um papel importante na forma como você atende aos requisitos de segurança, conforme discutido na Contas da AWS seção Benefícios de usar várias do whitepaper Organizando seu AWS ambiente usando várias contas. Por exemplo, você pode organizar suas cargas de trabalho em contas separadas e contas de grupo dentro de uma unidade organizacional (OU) com base na função, nos requisitos de conformidade ou em um conjunto comum de controles, em vez de espelhar a estrutura de relatórios da sua empresa. Lembre-se da segurança e da infraestrutura para permitir que sua empresa defina barreiras comuns à medida que suas cargas de trabalho crescem. Essa abordagem fornece limites e controles robustos entre cargas de trabalho. A separação em nível de conta, em combinação com AWS Organizations, é usada para isolar ambientes de produção dos ambientes de desenvolvimento e teste ou para fornecer um limite lógico forte entre cargas de trabalho que processam dados de diferentes classificações, como Payment Card Industry Data Security Standard (PCI DSS) ou Health Insurance Portability and Accountability Act (HIPAA). Embora você possa começar sua AWS jornada com uma única conta, AWS recomenda que você configure várias contas à medida que suas cargas de trabalho aumentam em tamanho e complexidade.

As permissões permitem que você especifique o acesso aos AWS recursos. As permissões são concedidas a entidades do IAM conhecidas como diretores (usuários, grupos e funções). Por padrão, os diretores começam sem permissões. Os diretores do IAM não podem fazer nada AWS até que você lhes conceda permissões, e você pode configurar grades de proteção que se apliquem

de forma tão ampla quanto toda a sua AWS organização ou de forma tão refinada quanto uma combinação individual de principal, ação, recurso e condições.

Usando AWS Organizations para segurança

> Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

AWS Organizationsajuda você a gerenciar e governar centralmente seu ambiente à medida que você cresce e escala seus AWS recursos. Ao usar AWS Organizations, você pode criar programaticamente novas contas Contas da AWS, alocar recursos, agrupar contas para organizar suas cargas de trabalho e aplicar políticas a contas ou grupos de contas para fins de governança. Uma AWS organização consolida as suas Contas da AWS para que você possa administrá-las como uma única unidade. Tem uma conta de gerenciamento junto com zero ou mais contas de membros. A maioria de suas cargas de trabalho reside em contas de membros, exceto alguns processos gerenciados centralmente que devem residir na conta de gerenciamento ou em contas designadas como administradores delegados, especificamente. Serviços da AWS Você pode fornecer ferramentas e acesso a partir de um local central para que sua equipe de segurança gerencie as necessidades de segurança em nome de uma AWS organização. Você pode reduzir a duplicação de recursos compartilhando recursos essenciais em sua AWS organização. Você pode agrupar contas em unidades AWS organizacionais (OUs), que podem representar ambientes diferentes com base nos requisitos e na finalidade da carga de trabalho. AWS Organizations também fornece várias políticas que permitem que você aplique centralmente controles de segurança adicionais a todas as contas dos membros em suas organizações. Esta seção se concentra nas políticas de controle de serviços (SCPs), nas políticas de controle de recursos (RCPs) e nas políticas declarativas.

Com AWS Organizations, você pode usar SCPse RCPsaplicar proteções de permissão no nível da AWS organização, da OU ou da conta. SCPs são proteções que se aplicam aos diretores na conta de uma organização, com exceção da conta de gerenciamento (que é um dos motivos para não executar cargas de trabalho nessa conta). Quando você anexa um SCP a uma OU, a SCP é herdada pela criança OUs e pelas contas dessa OU. SCPs não conceda nenhuma permissão. Em vez disso, eles especificam as permissões máximas disponíveis para seus diretores em uma AWS organização, UO ou conta. Você ainda precisa anexar políticas baseadas em identidade ou em recursos aos diretores ou recursos em sua conta para realmente conceder permissões Contas da AWS a eles.

Por exemplo, se um SCP negar acesso a todo o Amazon S3, um principal afetado pelo SCP não terá acesso ao Amazon S3, mesmo que tenha acesso explícito por meio de uma política do IAM. Para obter mais informações sobre como as políticas do IAM são avaliadas, a função e como o acesso é finalmente concedido ou negado, consulte Lógica de avaliação de políticas na documentação do IAM. SCPs

RCPs são barreiras que se aplicam aos recursos nas contas de uma organização, independentemente de os recursos pertencerem à mesma organização. Por exemplo SCPs, RCPs não afete os recursos na conta de gerenciamento e não conceda nenhuma permissão. Quando você anexa um RCP a uma OU, o RCP é herdado pelo filho OUs e pelas contas da OU. RCPs forneça controle central sobre o máximo de permissões disponíveis para recursos em sua organização e, atualmente, ofereça suporte a um subconjunto de Serviços da AWS. Ao projetar SCPs para o seu OUs, recomendamos que você avalie as alterações usando o simulador de políticas do IAM. Você também deve analisar os últimos dados acessados no IAM e usar AWS CloudTrail para registrar o uso do serviço no nível da API para entender o impacto potencial das alterações do SCP.

SCPs e RCPs são controles independentes. Você pode optar por habilitar somente SCPs ou RCPs usar os dois tipos de política juntos com base nos controles de acesso que você deseja aplicar. Por exemplo, se você quiser impedir que os diretores da sua organização acessem recursos fora da sua organização, aplique esse controle usando. SCPs Se você quiser restringir ou impedir que identidades externas acessem seus recursos, aplique esse controle usando. RCPs Para obter mais informações e casos de uso de RCPs e SCPs, consulte Usando SCPs e RCPs na AWS Organizations documentação.

Você pode usar políticas AWS Organizations declarativas para declarar e aplicar centralmente a configuração desejada para uma determinada empresa AWS service (Serviço da AWS) em grande escala em toda a organização. Por exemplo, você pode bloquear o acesso público à internet para recursos do Amazon VPC em toda a sua organização. Diferentemente das políticas de autorização, como SCPs e RCPs, as políticas declarativas são aplicadas no plano de controle AWS de um serviço. As políticas de autorização regulam o acesso ao APIs, enquanto as políticas declarativas são aplicadas diretamente no nível do serviço para impor uma intenção duradoura. Essas políticas ajudam a garantir que a configuração básica de an AWS service (Serviço da AWS) seja sempre mantida, mesmo quando o serviço introduz novos recursos ou. APIs A configuração básica também é mantida quando novas contas são adicionadas a uma organização ou quando novas entidades principais e recursos são criados. As políticas declarativas podem ser aplicadas a uma organização inteira ou a contas específicas OUs .

Cada um Conta da AWS tem um único usuário raiz que tem permissões completas para todos os AWS recursos por padrão. Como prática recomendada de segurança, recomendamos que você não use o usuário root, exceto para algumas tarefas que exigem explicitamente um usuário root. Se você gerencia vários Contas da AWS AWS Organizations, pode desabilitar centralmente o login root e, em seguida, realizar ações com privilégios root em nome de todas as contas dos membros. Depois de gerenciar centralmente o acesso raiz às contas dos membros, você pode excluir a senha do usuário raiz, as chaves de acesso e os certificados de assinatura, além de desativar a autenticação multifator (MFA) das contas dos membros. Novas contas criadas com acesso raiz gerenciado centralmente não têm credenciais de usuário raiz por padrão. As contas dos membros não podem fazer login com o usuário raiz nem realizar a recuperação da senha do usuário raiz.

AWS Control Toweroferece uma maneira simplificada de configurar e gerenciar várias contas. Ele automatiza a configuração de contas em sua AWS organização, automatiza o provisionamento, aplica controles (que incluem controles preventivos e de detetive) e fornece um painel para visibilidade. Uma política adicional de gerenciamento do IAM, um limite de permissões, é anexada a diretores específicos do IAM (usuários ou funções) e define as permissões máximas que uma política baseada em identidade pode conceder a um diretor do IAM.

AWS Organizations ajuda você a configurar Serviços da AWSque se aplicam a todas as suas contas. Por exemplo, você pode configurar o registro central de todas as ações realizadas em sua AWS organização usando CloudTrail e impedir que as contas dos membros desativem o registro. Você também pode agregar centralmente os dados das regras que você definiu usando AWS Config, para que você possa auditar suas cargas de trabalho para verificar a conformidade e reagir rapidamente às mudanças. Você pode usar AWS CloudFormation StackSetspara gerenciar centralmente CloudFormation as pilhas entre contas e OUs em sua AWS organização, para que você possa provisionar automaticamente uma nova conta para atender aos seus requisitos de segurança.

A configuração padrão dos AWS Organizations suportes usados SCPs como listas de negação. Usando uma estratégia de lista de negação, os administradores de contas de membros podem delegar todos os serviços e ações até que você crie e anexe um SCP que negue um serviço específico ou um conjunto de ações. As declarações de negação exigem menos manutenção do que uma lista de permissões, porque você não precisa atualizá-las ao AWS adicionar novos serviços. As declarações de negação geralmente têm caracteres mais curtos, então é mais fácil permanecer dentro do tamanho máximo SCPs. Em uma declaração em que o `Effect` elemento tem um valor de`Deny`, você também pode restringir o acesso a recursos específicos ou definir condições para quando SCPs estão em vigor. Por outro lado, uma `Allow` declaração em um SCP se aplica a

todos os recursos ("*") e não pode ser restringida por condições. Para obter mais informações e exemplos, consulte Estratégias para uso SCPs na AWS Organizations documentação.

Considerações sobre design

- Como alternativa, para usar SCPs como uma lista de permissões, você deve substituir o `FullAWSAccess` SCP gerenciado pela AWS por um SCP que permita explicitamente somente os serviços e ações que você deseja permitir. Para que uma permissão seja habilitada para uma conta específica, cada SCP (da raiz até cada OU no caminho direto para a conta e até mesmo anexado à própria conta) deve permitir essa permissão. Esse modelo é mais restritivo por natureza e pode ser adequado para cargas de trabalho altamente regulamentadas e sensíveis. Essa abordagem exige que você permita explicitamente cada serviço ou ação do IAM no caminho de Conta da AWS até a OU.
- Idealmente, você usaria uma combinação de estratégias de lista de negação e lista de permissões. Use a lista de permissões para definir a lista de Serviços da AWS aprovados permitidos para uso em uma AWS organização e anexe esse SCP na raiz da sua AWS organização. Se você tiver um conjunto diferente de serviços permitidos de acordo com seu ambiente de desenvolvimento, anexará os respectivos SCPs em cada UO. Em seguida, você pode usar a lista de negação para definir proteções corporativas negando explicitamente ações específicas do IAM.
- RCPs aplicam-se aos recursos de um subconjunto de. Serviços da AWS Para obter mais informações, consulte Lista Serviços da AWS desse suporte RCPs na AWS Organizations documentação. A configuração padrão dos AWS Organizations suportes usados RCPs como listas de negação. Quando você habilita RCPs em sua organização, uma política AWS gerenciada chamada `RCPFullAWSAccess` é automaticamente anexada à raiz da organização, a cada UO e a cada conta em sua organização. Você não pode desanexar essa política. Esse RCP padrão permite que todos os diretores e ações acessem a avaliação do RCP. Isso significa que, até você começar a criar e anexar RCPs, todas as suas permissões atuais do IAM continuarão funcionando da mesma forma. Essa política AWS gerenciada não concede acesso. Em seguida, você pode criar uma nova RCPs como uma lista de declarações de negação para bloquear o acesso aos recursos em sua organização.

A conta de gerenciamento, o acesso confiável e os administradores delegados

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

A conta de gerenciamento (também chamada de conta de gerenciamento da AWS organização ou conta de gerenciamento da organização) é exclusiva e diferenciada de todas as outras contas em AWS Organizations. É a conta que cria a AWS organização. Nessa conta, você pode criar Contas da AWS na AWS organização, convidar outras contas existentes para a AWS organização (ambos os tipos são considerados contas membros), remover contas da AWS organização e aplicar políticas do IAM à raiz ou às contas dentro da AWS organização. OUs

A conta de gerenciamento implanta proteções de segurança universais por meio SCPs de implantações de serviços (como CloudTrail) que afetarão todas as contas membros da organização. RCPs AWS Para restringir ainda mais as permissões na conta de gerenciamento, essas permissões podem ser delegadas a outra conta apropriada, como uma conta de segurança, sempre que possível.

A conta de gerenciamento tem as responsabilidades de uma conta pagadora e é responsável pelo pagamento de todos as cobranças que são acumuladas pelas contas-membro. Você não pode trocar a conta de gerenciamento de uma AWS organização. Um só Conta da AWS pode ser membro de uma AWS organização por vez.

Devido à funcionalidade e ao escopo de influência que a conta de gerenciamento tem, recomendamos que você limite o acesso a essa conta e conceda permissões somente às funções que precisam delas. Dois recursos que ajudam você a fazer isso são acesso confiável e administrador delegado. Você pode usar o acesso confiável para permitir AWS service (Serviço da AWS) que um que você especifique, chamado de serviço confiável, execute tarefas em sua AWS organização e em suas contas em seu nome. Isso requer a concessão de permissões ao serviço confiável, mas não afeta de outra forma as permissões para usuários ou funções do IAM. Você pode usar o acesso confiável para especificar as configurações e os detalhes de configuração que você gostaria que o serviço confiável mantivesse nas contas da sua AWS organização em seu nome. Por exemplo, a seção de contas de gerenciamento da organização do AWS SRA explica como conceder ao CloudTrail serviço acesso confiável para criar uma trilha CloudTrail organizacional em todas as contas AWS da sua organização.

Alguns Serviços da AWS oferecem suporte ao recurso de administrador delegado no AWS Organizations. Com esse recurso, os serviços compatíveis podem registrar uma conta de AWS membro na AWS organização como administrador das contas da AWS organização nesse serviço. Esse recurso fornece flexibilidade para diferentes equipes em sua empresa usarem contas separadas, conforme apropriado para suas responsabilidades, para gerenciar Serviços da AWS todo o ambiente. Os serviços AWS de segurança no AWS SRA que atualmente oferecem suporte ao administrador delegado incluem o IAM Identity Center,, AWS Config, AWS Firewall Manager Amazon GuardDuty, IAM Access Analyzer, Amazon Macie, AWS Security Hub Cloud Security Posture Management (),AWS Security Hub CSPM Amazon Detective, Amazon Inspector e. AWS Audit Manager AWS Systems Manager O uso do recurso de administrador delegado é enfatizado na AWS SRA como uma prática recomendada, e delegamos a administração de serviços relacionados à segurança à conta do Security Tooling.

Estrutura de contas dedicada

> Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

E Conta da AWS fornece limites de segurança, acesso e cobrança para seus AWS recursos e permite que você alcance independência e isolamento de recursos. Por padrão, nenhum acesso é permitido entre contas.

Ao projetar sua OU e estrutura de contas, comece com a segurança e a infraestrutura em mente. Recomendamos criar um conjunto básico OUs para essas funções específicas, dividido em Infraestrutura e Segurança OUs. Essas recomendações de UO e de contas abrangem um subconjunto de nossas diretrizes mais amplas AWS Organizations e abrangentes para o design da estrutura de várias contas. Para obter um conjunto completo de recomendações, consulte Organizando seu AWS ambiente usando várias contas na AWS documentação e na postagem do blog Melhores práticas para unidades organizacionais com AWS Organizations.

O AWS SRA utiliza as seguintes contas para realizar operações de segurança eficazes em. AWS Essas contas dedicadas ajudam a garantir a separação de tarefas, oferecem suporte a diferentes políticas de governança e acesso para diferentes tipos de aplicativos e dados e ajudam a mitigar o impacto de um evento de segurança. Nas discussões a seguir, nos concentraremos nas contas de produção (produção) e nas cargas de trabalho associadas. As contas do ciclo de vida de desenvolvimento de software (SDLC) (geralmente chamadas de contas de desenvolvimento e

teste) são destinadas à preparação de resultados e podem operar sob um conjunto de políticas de segurança diferente das contas de produção.

Conta	OU	Função de segurança
Gerenciamento	—	Governança central e gerenciamento de tudo Regiões da AWS e contas. Conta da AWS Aquele que hospeda a raiz da AWS organização.
Ferramentas de segurança	Segurança	Dedicado Contas da AWS para operar serviços de segurança amplamente aplicáveis (como Security Hub CSPM GuardDuty, Audit Manager, Detective, Amazon Inspector AWS Config e), Contas da AWS monitorar e automatizar alertas e respostas de segurança. (Em AWS Control Tower, o nome padrão da conta na OU de segurança é Conta de auditoria.)
Arquivo de log	Segurança	Dedicado Contas da AWS à ingestão e arquivamento de todos os registros e backups de todos e. Regiões da AWS Contas da AWS Isso deve ser projetado como armazenamento imutável.
Rede	Infraestrutura	O gateway entre seu aplicativo e a Internet em geral. A conta

		de rede isola os serviços, a configuração e a operação de rede mais amplos das cargas de trabalho de aplicativos individuais, da segurança e de outras infraestruturas.
Serviços compartilhados	Infraestrutura	Essa conta oferece suporte aos serviços que vários aplicativos e equipes usam para fornecer seus resultados. Os exemplos incluem serviços de diretório do Identity Center (Active Directory), serviços de mensagens e serviços de metadados.
Aplicação	Workloads	Contas da AWS que hospedam os aplicativos da AWS organização e executam as cargas de trabalho. (Às vezes, são chamadas de contas de carga de trabalho.) As contas de aplicativos devem ser criadas para isolar os serviços de software em vez de serem mapeadas para suas equipes. Isso torna o aplicativo implantado mais resiliente às mudanças organizacionais.

AWS organização e estrutura de contas da AWS SRA

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

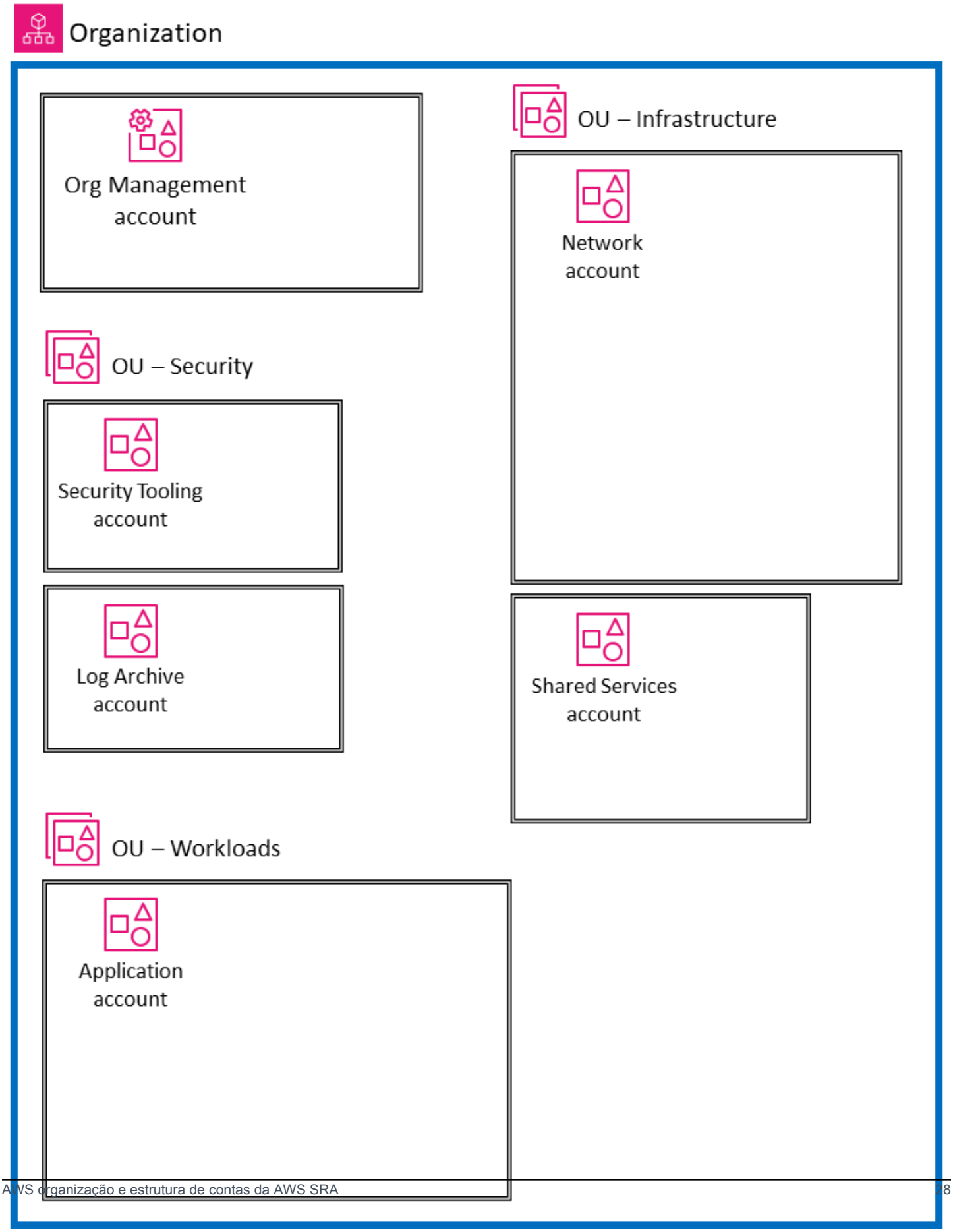
O diagrama a seguir captura a estrutura de alto nível do AWS SRA sem exibir serviços específicos. Ela reflete a estrutura de contas dedicada discutida na seção anterior, e incluímos o diagrama aqui para orientar a discussão em torno dos componentes principais da arquitetura:

- Todas as contas mostradas no diagrama fazem parte de uma única AWS organização.
- No canto superior esquerdo do diagrama está a conta de gerenciamento da organização, usada para criar a AWS organização.
- Abaixo da conta de gerenciamento da organização está a OU de segurança com duas contas específicas: uma para o Security Tooling e outra para o Log Archive.
- No lado direito está a UO de Infraestrutura com a conta de Rede e a conta de Serviços Compartilhados.
- Na parte inferior do diagrama está a UO de cargas de trabalho, que está associada a uma conta de aplicativo que abriga o aplicativo corporativo.

Para essa orientação, todas as contas são consideradas contas de produção (produção) que operam em uma única Região da AWS. A maioria Serviços da AWS (exceto os serviços globais) tem escopo regional, o que significa que os planos de controle e dados do serviço existem de forma independente em cada um. Região da AWS Por esse motivo, você deve replicar essa arquitetura em tudo o Regiões da AWS que planeja usar, para garantir a cobertura de toda a AWS paisagem. Se você não tiver nenhuma carga de trabalho em uma região específica Região da AWS, desative a região usando SCPsou usando mecanismos de registro e monitoramento. Você pode usar o Security Hub CSPM para agregar descobertas e pontuações de segurança de várias Regiões da AWS para uma única região de agregação para visibilidade centralizada.

Ao hospedar uma AWS organização com um grande conjunto de contas, é vantajoso ter uma camada de orquestração que facilite a implantação e a governança da conta. AWS Control Tower oferece uma maneira simples de configurar e controlar um AWS ambiente com várias contas. As amostras de código AWS SRA no GitHub repositório demonstram como você pode usar a solução

Customizations for AWS Control Tower (cFCT) para implantar estruturas recomendadas pela SRA. AWS

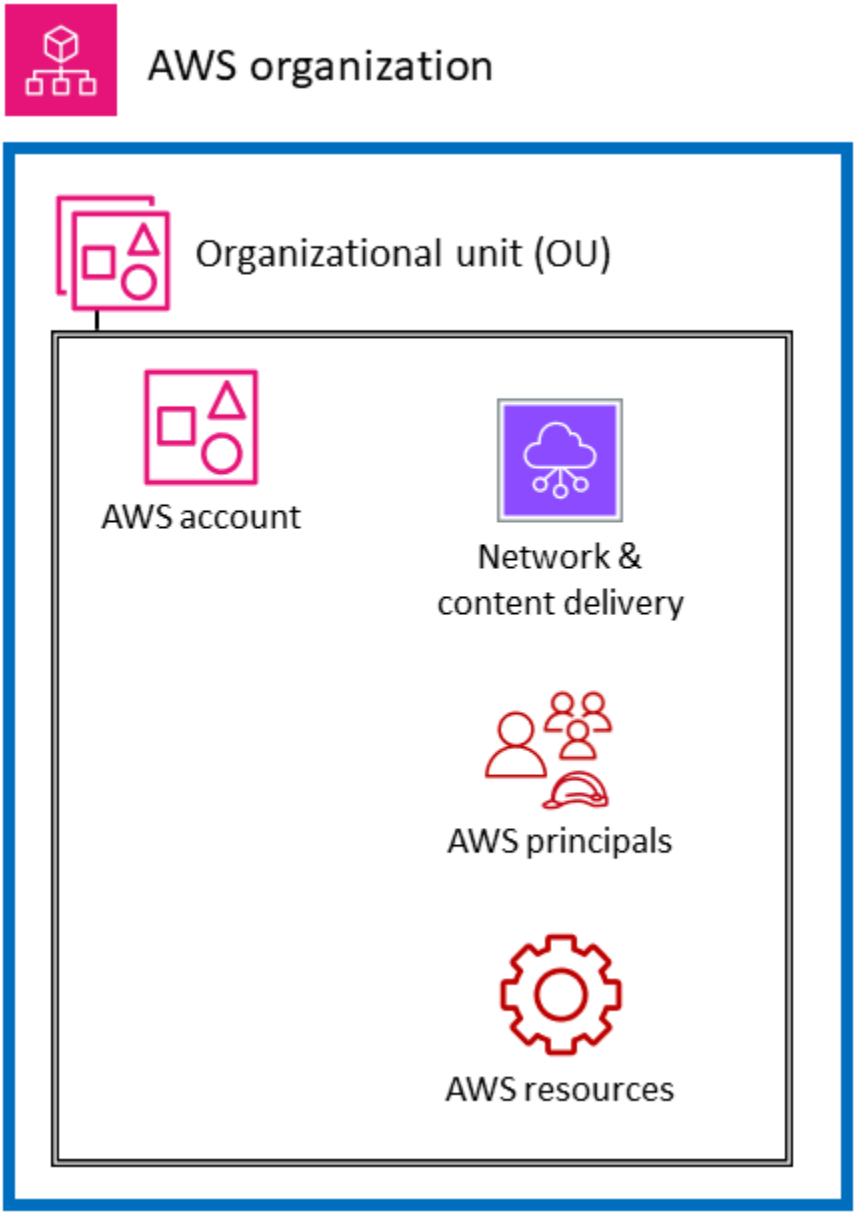

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

Aplique serviços de segurança em toda a sua AWS organização

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Conforme descrito na seção anterior, os clientes estão procurando uma forma adicional de pensar e organizar estrategicamente o conjunto completo de serviços de AWS segurança. Atualmente, a abordagem organizacional mais comum é agrupar os serviços de segurança por função principal, de acordo com o que cada serviço faz. A perspectiva de segurança do AWS CAF lista nove recursos funcionais, incluindo gerenciamento de identidade e acesso, proteção de infraestrutura, proteção de dados e detecção de ameaças. Serviços da AWS Combinar esses recursos funcionais é uma forma prática de tomar decisões de implementação em cada área. Por exemplo, ao analisar o gerenciamento de identidade e acesso, o IAM e o IAM Identity Center são serviços a serem considerados. Ao arquitetar sua abordagem de detecção de ameaças, GuardDuty pode ser sua primeira consideração.

Como complemento a essa visão funcional, você também pode visualizar sua segurança com uma visão transversal e estrutural. Ou seja, além de perguntar: “O que Serviços da AWS devo usar para controlar e proteger minhas identidades, acesso lógico ou mecanismos de detecção de ameaças?” , você também pode perguntar: “O que Serviços da AWS devo aplicar em toda a minha AWS organização? Quais são as camadas de defesa que eu deveria implementar para proteger as instâncias do Amazon EC2 no centro do meu aplicativo?” Nesta visualização, você mapeia Serviços da AWS e feições para camadas em seu AWS ambiente. Alguns serviços e recursos são ideais para implementar controles em toda a organização da AWS . Por exemplo, bloquear o acesso público aos buckets do Amazon S3 é um controle específico nessa camada. De preferência, isso deve ser feito na organização raiz, em vez de fazer parte da configuração da conta individual. Outros serviços e recursos são melhor usados para ajudar a proteger recursos individuais em um Conta da AWS. A implementação de uma autoridade de certificação (CA) subordinada em uma conta que exige certificados TLS privados é um exemplo dessa categoria. Outro agrupamento igualmente importante consiste em serviços que afetam a camada de rede virtual da sua AWS infraestrutura. O diagrama a seguir mostra seis camadas em um AWS ambiente típico: AWS organização, unidade organizacional (OU), conta, infraestrutura de rede, diretores e recursos.



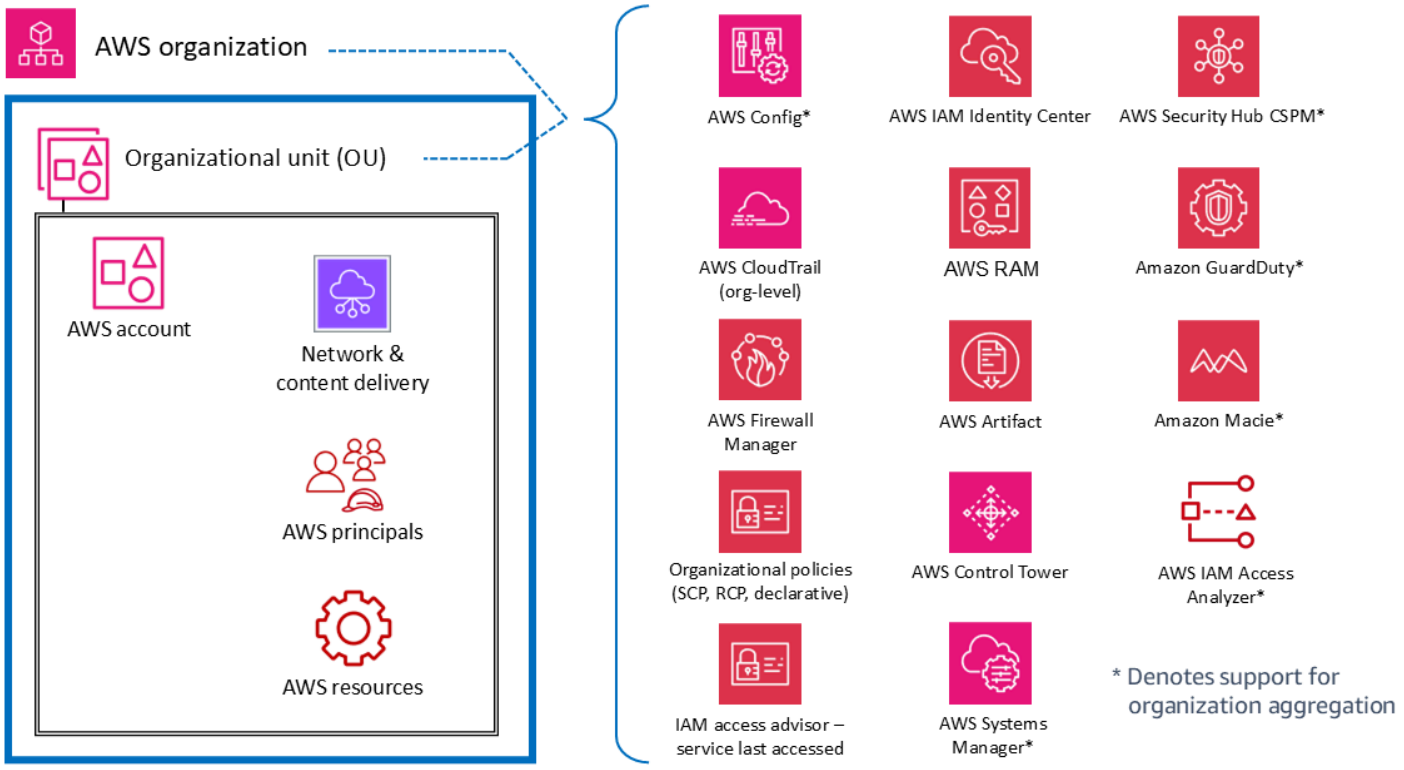
Compreender os serviços nesse contexto estrutural, incluindo os controles e proteções em cada camada, ajuda você a planejar e implementar uma defense-in-depth estratégia em todo o seu AWS ambiente. Com essa perspectiva, você pode responder a perguntas de cima para baixo (por exemplo, “Quais serviços estou usando para implementar controles de segurança em toda a minha AWS organização?”) e de baixo para cima (por exemplo, “Quais serviços gerenciam controles nesta instância do EC2?”). Nesta seção, examinamos os elementos de um AWS ambiente e identificamos os serviços e recursos de segurança associados. Obviamente, alguns Serviços da AWS têm amplos conjuntos de recursos e oferecem suporte a vários objetivos de segurança. Esses serviços podem oferecer suporte a vários elementos do seu AWS ambiente.

Para maior clareza, fornecemos breves descrições de como alguns dos serviços atendem aos objetivos declarados. A próxima seção fornece uma discussão mais aprofundada sobre os serviços individuais em cada um Conta da AWS.

Contas múltiplas ou em toda a organização

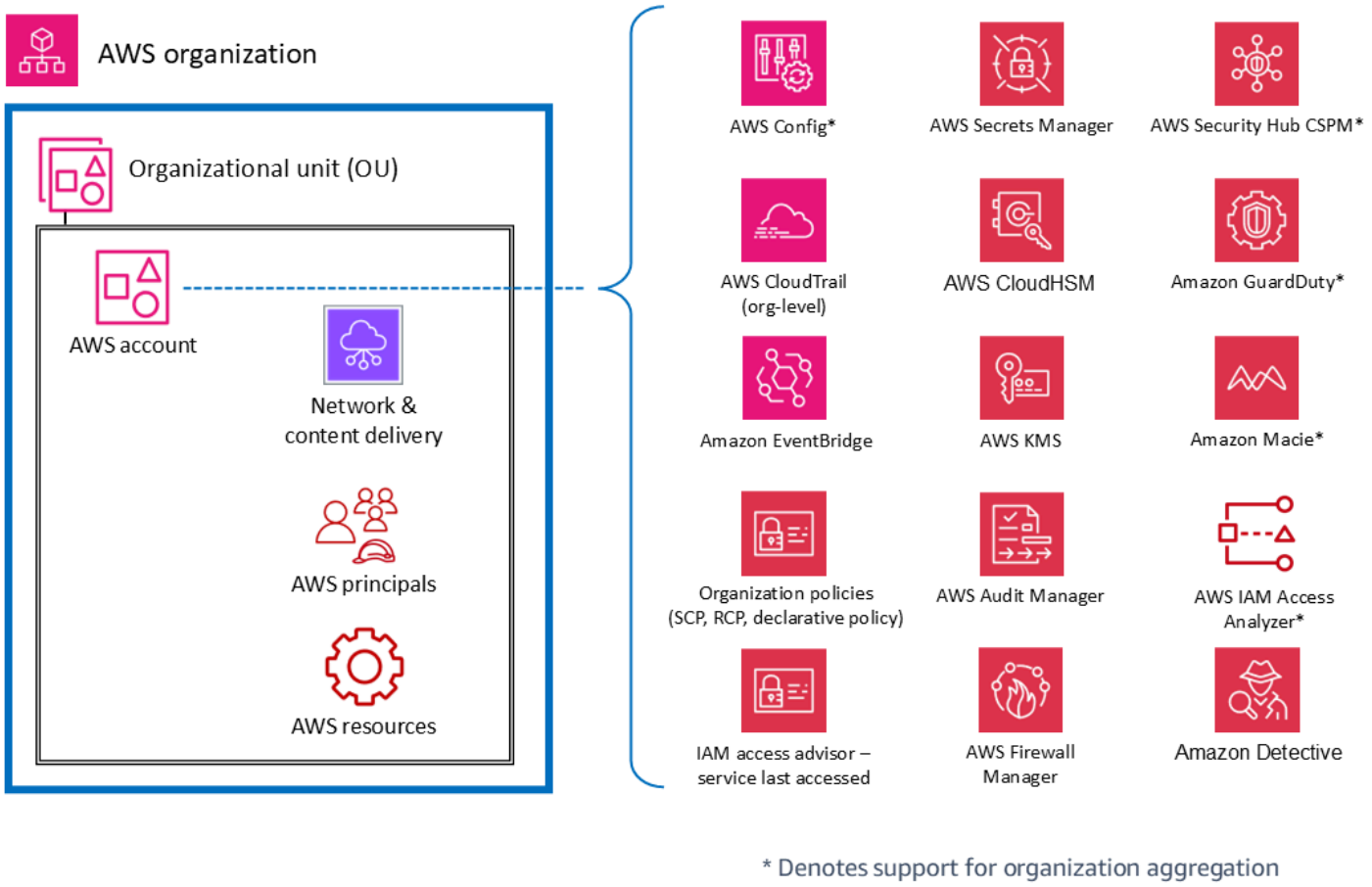
No nível superior, existem Serviços da AWS recursos projetados para aplicar recursos de governança e controle ou barreiras em várias contas em uma AWS organização (incluindo toda a organização ou específicas OUs). As políticas de controle de serviço (SCPs) e as políticas de controle de recursos (RCPs) são bons exemplos de recursos do IAM que fornecem proteções preventivas em toda a AWS organização. AWS Organizations também fornece uma política declarativa que define e impõe centralmente a configuração de linha de base para em grande escala. Serviços da AWS Outro exemplo é CloudTrail, que fornece monitoramento por meio de uma trilha organizacional que registra todos os eventos de todos Contas da AWS nessa AWS organização. Essa trilha abrangente é diferente das trilhas individuais que podem ser criadas em cada conta. Um terceiro exemplo é AWS Firewall Manager o que você pode usar para configurar, aplicar e gerenciar vários recursos em todas as contas da sua AWS organização: AWS WAF regras, regras AWS WAF clássicas, AWS Shield Advanced proteções, grupos AWS Network Firewall de segurança, políticas Amazon Route 53 Resolver e políticas de firewall de DNS da Amazon Virtual Private Cloud (Amazon VPC).

Os serviços marcados com um asterisco (*) no diagrama a seguir operam com um escopo duplo: em toda a organização e focado na conta. Esses serviços basicamente monitoram ou ajudam a controlar a segurança em uma conta individual. No entanto, eles também oferecem suporte à capacidade de agregar os resultados de várias contas em uma conta de toda a organização para visibilidade e gerenciamento centralizados. Para maior clareza, considere SCPs a possibilidade de aplicar em toda uma UO ou AWS organização. Conta da AWS Por outro lado, você pode configurar e gerenciar GuardDuty tanto no nível da conta (onde as descobertas individuais são geradas) quanto no nível da AWS organização (usando o recurso de administrador delegado), onde as descobertas podem ser visualizadas e gerenciadas de forma agregada.



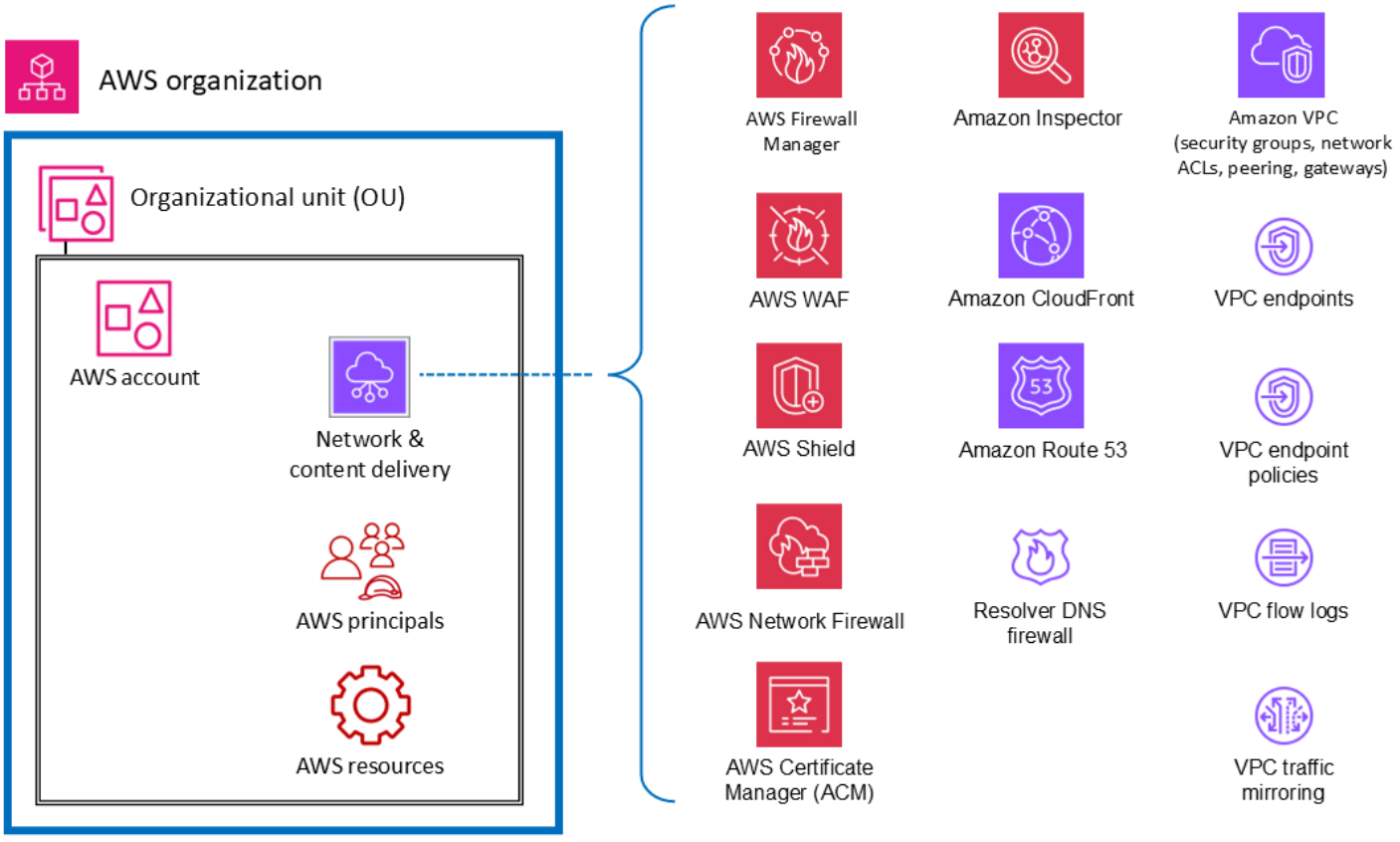
AWS contas

Dentro OUs, existem serviços que ajudam a proteger vários tipos de elementos em um Conta da AWS. Por exemplo, geralmente AWS Secrets Manager é gerenciado a partir de uma conta específica e protege recursos (como credenciais de banco de dados ou informações de autenticação), aplicativos e Serviços da AWS nessa conta. O IAM Access Analyzer pode ser configurado para gerar descobertas quando recursos especificados são acessíveis por diretores fora do. Conta da AWS Conforme mencionado na seção anterior, muitos desses serviços também podem ser configurados e administrados internamente AWS Organizations, para que possam ser gerenciados em várias contas. Esses serviços estão marcados com um asterisco (*) no diagrama. Eles também facilitam a agregação de resultados de várias contas e a entrega desses resultados em uma única conta. Isso dá às equipes de aplicativos individuais a flexibilidade e a visibilidade para gerenciar as necessidades de segurança específicas de sua carga de trabalho, além de permitir governança e visibilidade às equipes de segurança centralizadas. GuardDuty é um exemplo desse serviço. GuardDuty monitora recursos e atividades associados a uma única conta, e GuardDuty as descobertas de várias contas de membros (como todas as contas em uma AWS organização) podem ser coletadas, visualizadas e gerenciadas a partir de uma conta de administrador delegado.



Rede virtual, computação e entrega de conteúdo

Como o acesso à rede é muito importante em termos de segurança e a infraestrutura computacional é um componente fundamental de muitas AWS cargas de trabalho, há muitos serviços e recursos de AWS segurança dedicados a esses recursos. Por exemplo, o Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas AWS cargas de trabalho em busca de vulnerabilidades. Essas verificações incluem verificações de acessibilidade de rede que indicam que há caminhos de rede permitidos para instâncias do Amazon EC2 em seu ambiente. A Amazon VPC permite que você defina uma rede virtual na qual você pode lançar AWS recursos. Essa rede virtual se assemelha muito a uma rede tradicional e inclui uma variedade de recursos e benefícios. Os VPC endpoints permitem que você conecte sua VPC de forma privada aos serviços compatíveis Serviços da AWS e aos serviços de endpoint fornecidos por eles, AWS PrivateLink sem precisar de um caminho para a Internet. O diagrama a seguir ilustra os serviços de segurança que se concentram na infraestrutura de rede, computação e entrega de conteúdo.



Diretores e recursos

AWS diretores e AWS recursos (junto com as políticas do IAM) são os elementos fundamentais no gerenciamento de identidade e acesso em AWS. Um principal autenticado AWS pode realizar ações e acessar AWS recursos. Um principal pode ser autenticado como usuário Conta da AWS raiz e usuário do IAM, ou assumindo uma função.

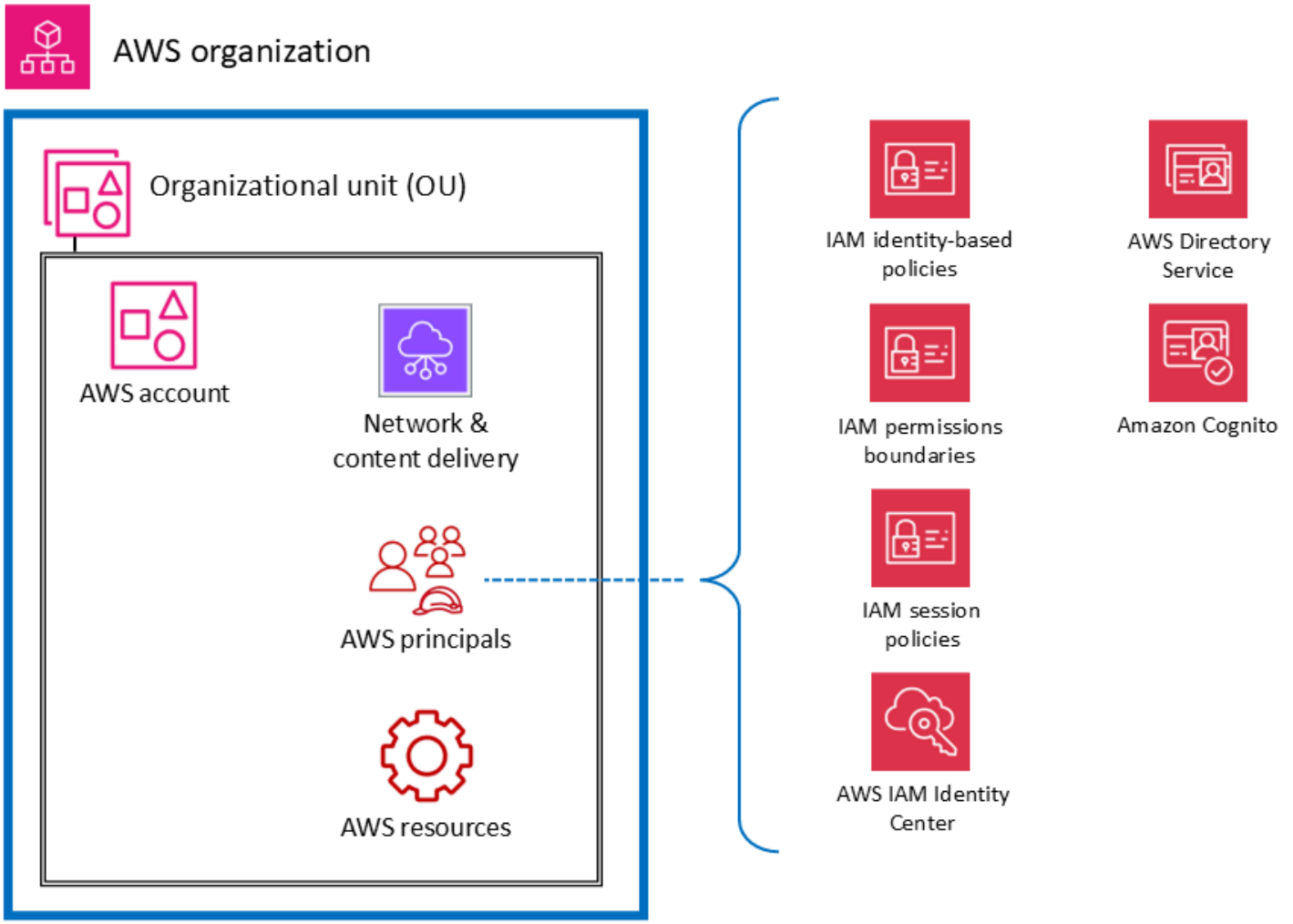
> **Note**
>
> Não crie chaves de API persistentes associadas à conta do usuário AWS raiz. O acesso à conta do usuário raiz deve ser limitado somente às tarefas que exigem um usuário raiz e somente por meio de um rigoroso processo de exceção e aprovação. Para ver as melhores práticas para proteger o usuário raiz da sua conta, consulte a documentação do IAM.

Um AWS recurso é um objeto que existe dentro de um AWS service (Serviço da AWS) com o qual você pode trabalhar. Os exemplos incluem uma instância do EC2, uma CloudFormation pilha, um tópico do Amazon Simple Notification Service (Amazon SNS) e um bucket do S3. As políticas do

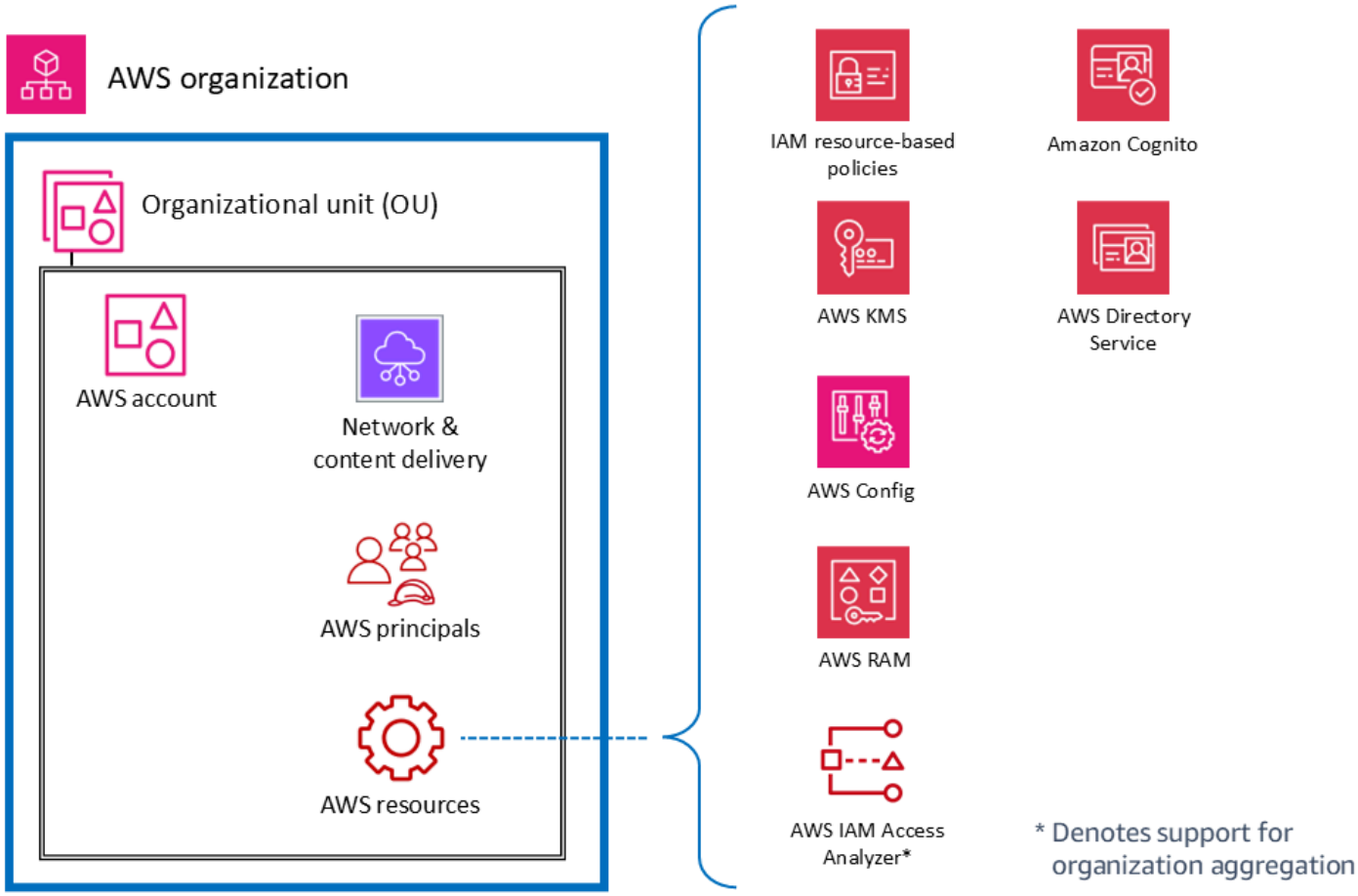
IAM são objetos que definem permissões quando são associadas a um principal (usuário, grupo ou função) ou AWS recurso do IAM. Políticas baseadas em identidade são documentos de política que você anexa a um diretor (funções, usuários e grupos de usuários) para controlar quais ações um diretor pode realizar, em quais recursos e sob quais condições. Políticas baseadas em recursos são documentos de política que você anexa a um recurso, como um bucket do S3. Essas políticas concedem ao principal especificado permissão para realizar ações específicas nesse recurso e definem as condições dessa permissão. As políticas baseadas em recursos são políticas em linha. A seção de recursos do IAM se aprofunda nos tipos de políticas do IAM e em como elas são usadas.

Para simplificar as coisas nessa discussão, listamos serviços e recursos de AWS segurança para diretores do IAM que têm como objetivo principal operar ou se candidatar aos diretores de contas. Mantemos essa simplicidade e, ao mesmo tempo, reconhecemos a flexibilidade e a amplitude dos efeitos das políticas de permissão do IAM. Uma única declaração em uma política pode ter efeitos em vários tipos de AWS entidades. Por exemplo, embora uma política baseada em identidade do IAM esteja associada a um principal do IAM e defina permissões (permitir, negar) para esse principal, a política também define implicitamente as permissões para as ações, recursos e condições especificados. Dessa forma, uma política baseada em identidade pode ser um elemento crítico na definição de permissões para um recurso.

O diagrama a seguir ilustra os serviços e recursos de AWS segurança para AWS diretores. As políticas baseadas em identidade são anexadas a um usuário, grupo ou função do IAM. Essas políticas permitem que você especifique o que cada identidade pode fazer (suas respectivas permissões). Uma política de sessão do IAM é uma política de permissões em linha que os usuários passam na sessão quando assumem a função. Você mesmo pode passar a política ou configurar seu agente de identidade para inserir a política quando suas identidades forem federadas. AWS Isso permite que seus administradores reduzam o número de funções que precisam criar, porque vários usuários podem assumir a mesma função, mas têm permissões de sessão exclusivas. O serviço IAM Identity Center é integrado às operações de AWS API AWS Organizations e ajuda você a gerenciar o acesso ao SSO e as permissões de usuário em toda a sua entrada Contas da AWS . AWS Organizations



O diagrama a seguir ilustra os serviços e recursos dos recursos da conta. Políticas baseadas em recurso são anexadas a um recurso. Por exemplo, você pode anexar políticas baseadas em recursos a buckets do S3, filas do Amazon Simple Queue Service (Amazon SQS), endpoints de VPC e chaves de criptografia. AWS KMS Você pode usar políticas baseadas em recursos para especificar quem tem acesso ao recurso e quais ações eles podem realizar nele. Políticas de bucket do S3, políticas de AWS KMS chaves e políticas de VPC endpoint são tipos de políticas baseadas em recursos. O IAM Access Analyzer ajuda você a identificar os recursos em sua organização e suas contas, como buckets do S3 ou funções do IAM, que são compartilhados com uma entidade externa. Isso permite identificar o acesso não intencional aos seus recursos e dados, o que é um risco de segurança. AWS Config permite que você avalie, audite e avalie as configurações dos AWS recursos suportados em seu Contas da AWS. AWS Config monitora e registra continuamente as configurações AWS dos recursos e avalia automaticamente as configurações gravadas em relação às configurações desejadas.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

A arquitetura AWS de referência de segurança

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra o AWS SRA. Esse diagrama arquitetônico reúne todos os serviços AWS relacionados à segurança. Ele é construído em torno de uma arquitetura web simples de três camadas que pode caber em uma única página. Nessa carga de trabalho, há uma camada da web por meio da qual os usuários se conectam e interagem com a camada do aplicativo, que lida com a lógica comercial real do aplicativo: recebendo entradas do usuário, fazendo alguns cálculos e gerando saídas. A camada do aplicativo armazena e recupera informações da camada de dados. A arquitetura é propositalmente modular e fornece abstração de alto nível para muitos aplicativos web modernos.

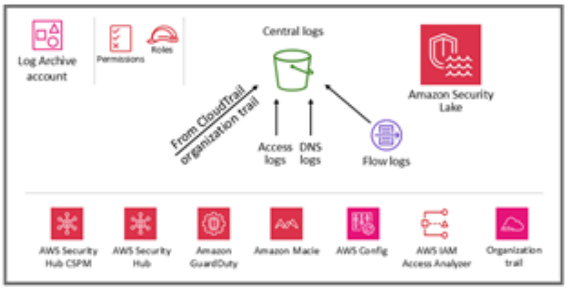
Diagramas de arquitetura

Para personalizar os diagramas de arquitetura de referência neste guia com base nas necessidades de sua empresa, você pode baixar o seguinte arquivo.zip e extrair seu conteúdo.

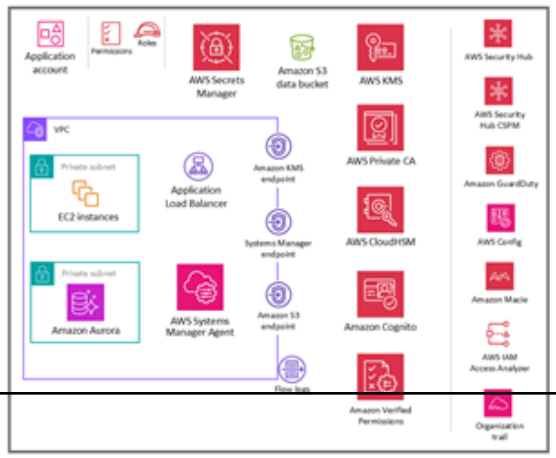
Baixe o arquivo de origem do diagrama (PowerPoint formato Microsoft)

Organization

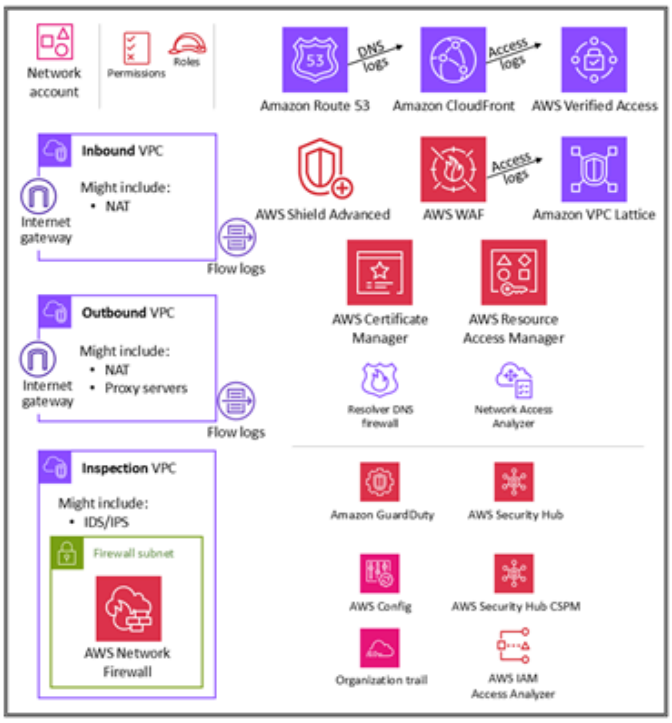
OU – Security

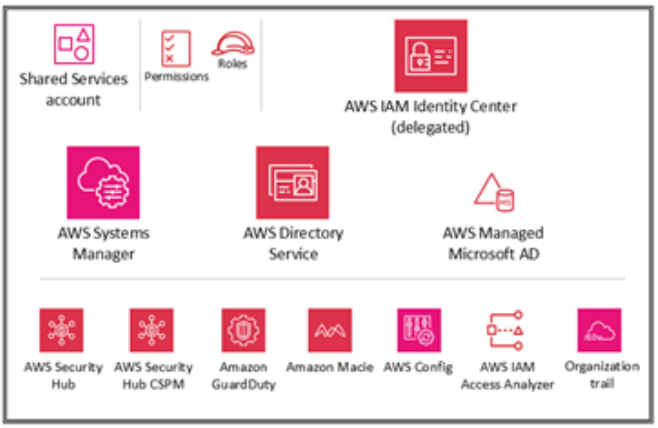


OU – Workloads



OU – Infrastructure





Para essa arquitetura de referência, o aplicativo web real e o nível de dados são deliberadamente representados da forma mais simples possível, por meio de EC2 instâncias da Amazon e de um banco de dados Amazon Aurora, respectivamente. A maioria dos diagramas de arquitetura se concentra e se aprofunda na Web, nos aplicativos e nas camadas de dados. Para facilitar a leitura, eles geralmente omitem os controles de segurança. Esse diagrama inverte essa ênfase para mostrar a segurança sempre que possível e mantém os níveis de aplicativos e dados tão simples quanto necessário para mostrar os recursos de segurança de forma significativa.

O AWS SRA contém todos os serviços AWS relacionados à segurança disponíveis no momento da publicação. (Veja o histórico do documento.) No entanto, nem toda carga de trabalho ou ambiente, com base em sua exposição exclusiva a ameaças, precisa implantar todos os serviços de segurança. Nosso objetivo é fornecer uma referência para uma variedade de opções, incluindo descrições de como esses serviços se encaixam arquitetonicamente, para que sua empresa possa tomar as decisões mais adequadas às suas necessidades de infraestrutura, carga de trabalho e segurança, com base no risco.

As seções a seguir examinam cada UO e cada conta para entender seus objetivos e os serviços AWS de segurança individuais associados a elas. Para cada elemento (normalmente um AWS service (Serviço da AWS)), este documento fornece as seguintes informações:

- Breve visão geral do elemento e sua finalidade de segurança no AWS SRA. Para obter descrições mais detalhadas e informações técnicas sobre serviços individuais, consulte o apêndice.
- Posicionamento recomendado para habilitar e gerenciar o serviço com mais eficiência. Isso é capturado nos diagramas de arquitetura individuais de cada conta e UO.
- Links de configuração, gerenciamento e compartilhamento de dados para outros serviços de segurança. Como esse serviço depende ou oferece suporte a outros serviços de segurança?
- Considerações de design. Primeiro, o documento destaca recursos ou configurações opcionais que têm implicações de segurança importantes. Segundo, quando a experiência de nossas equipes inclui variações comuns nas recomendações que fazemos, normalmente como resultado de requisitos ou restrições alternativas, o documento descreve essas opções.

OUs e contas

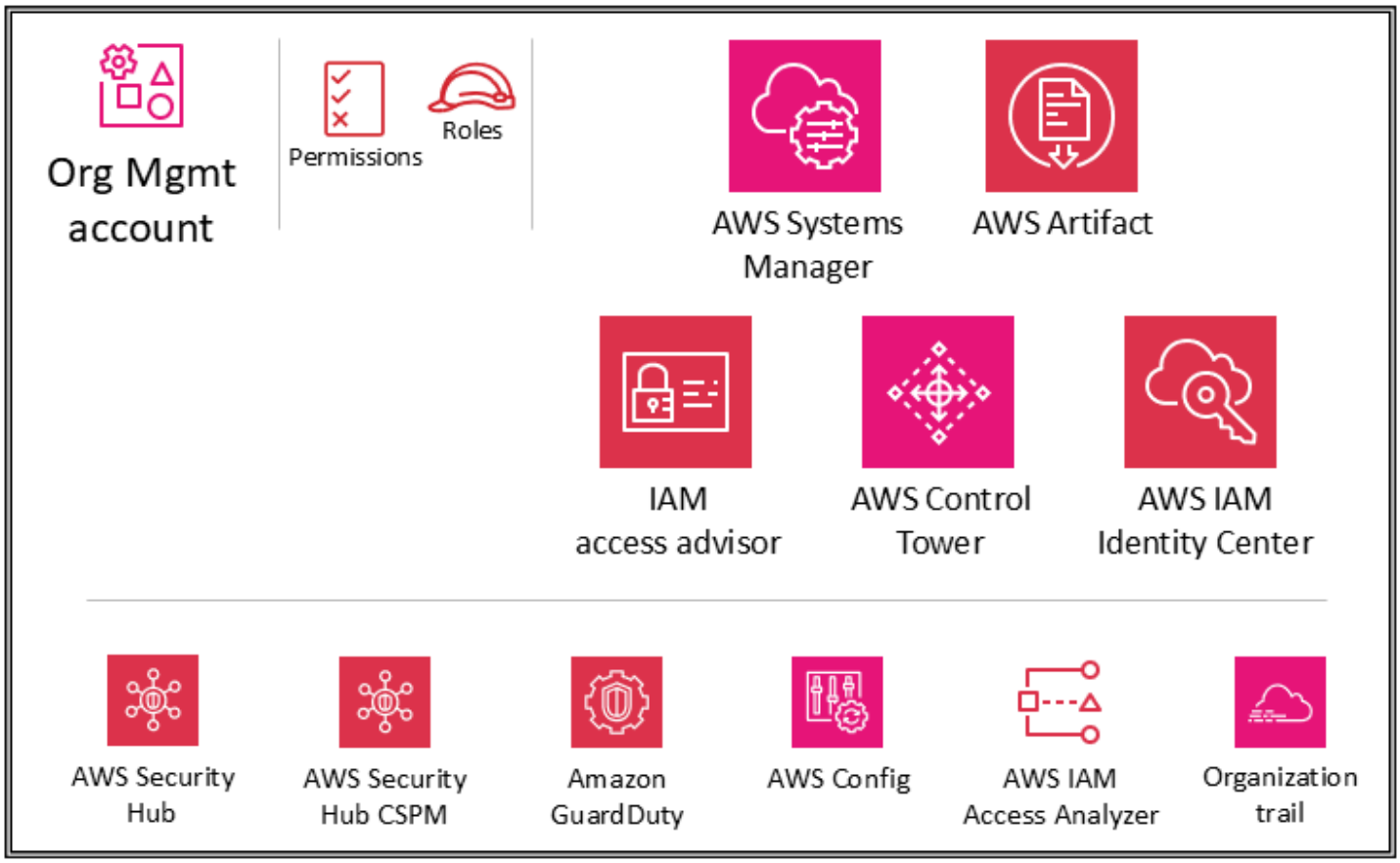
- Conta gerencial da organização
- UO de segurança | Conta do Security Tooling
- UO de segurança | Conta do Log Archive
- Infraestrutura de UO: conta de Rede

- Infraestrutura OU — conta de serviços compartilhados
- Workloads OU — Conta de aplicativo

Conta gerencial da organização

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços AWS de segurança configurados na conta de gerenciamento da organização.



As seções Usando AWS Organizations para segurança e A conta de gerenciamento, acesso confiável e administradores delegados anteriormente neste guia discutiram detalhadamente a finalidade e os objetivos de segurança da conta de gerenciamento da organização. Siga as melhores práticas de segurança para sua conta de gerenciamento de organizações. Isso inclui usar um endereço de e-mail gerenciado pela sua empresa, manter as informações de contato administrativas

e de segurança corretas (como anexar um número de telefone à conta no caso de AWS precisar entrar em contato com o proprietário da conta), habilitar a autenticação multifator (MFA) para todos os usuários e revisar regularmente quem tem acesso à conta de gerenciamento organizacional. Os serviços implantados na conta de gerenciamento da organização devem ser configurados com funções, políticas de confiança e outras permissões apropriadas para que os administradores desses serviços (que devem acessá-los na conta de gerenciamento da organização) também não possam acessar outros serviços de forma inadequada.

Políticas de controle de serviço

Com AWS Organizations, você pode gerenciar centralmente as políticas em várias Contas da AWS. Por exemplo, você pode aplicar políticas de controle de serviço (SCPs) em vários Contas da AWS membros de uma organização. SCPs permitem que você defina o que AWS service (Serviço da AWS) APIs pode e o que não pode ser executado pelos diretores do IAM (como usuários e funções do IAM) no membro Contas da AWS da sua organização. SCPs são criados e aplicados a partir da conta de gerenciamento da organização, Conta da AWS que é a que você usou quando criou sua organização. Leia mais sobre isso SCPs na seção Usando AWS Organizations para fins de segurança, anteriormente nesta referência.

Se você usa AWS Control Tower para gerenciar sua AWS organização, ele implantará um conjunto de SCPs proteções preventivas (categorizadas como obrigatórias, altamente recomendadas ou eletivas). Essas grades de proteção ajudam você a controlar seus recursos aplicando controles de segurança em toda a organização. Eles usam SCPs automaticamente uma aws-control-tower tag que tem um valor de managed-by-control-tower.

> **Considerações sobre design**
>
> SCPs afetam somente as contas dos membros na AWS organização. Embora sejam aplicados a partir da conta de gerenciamento da organização, eles não têm efeito sobre os usuários ou as funções dessa conta. Para saber mais sobre como a lógica de avaliação do SCP funciona e ver exemplos de estruturas recomendadas, consulte a postagem do AWS blog Como usar políticas de controle de serviço em AWS Organizations.

Políticas de controle de recursos

As políticas de controle de recursos (RCPs) oferecem controle centralizado sobre o máximo de permissões disponíveis para recursos em sua organização. Um RCP define uma barreira de

permissões ou define limites para as ações que as identidades podem realizar em relação aos recursos em sua organização. Você pode usar RCPs para restringir quem pode acessar seus recursos e impor requisitos sobre como seus recursos podem ser acessados no membro Contas da AWS da sua organização. Você pode se vincular RCPs diretamente a contas individuais ou à raiz da organização. OUs Para obter uma explicação detalhada de como RCPs funciona, consulte a avaliação do RCP na AWS Organizations documentação. Leia mais sobre isso RCPs na seção Usando AWS Organizations para fins de segurança, anteriormente nesta referência.

Se você usar AWS Control Tower para gerenciar sua AWS organização, ele implantará um conjunto de proteções preventivas (categorizadas RCPs como obrigatórias, altamente recomendadas ou eletivas). Essas grades de proteção ajudam você a controlar seus recursos aplicando controles de segurança em toda a organização. Eles usam SCPs automaticamente uma `aws-control-tower` tag que tem um valor de`managed-by-control-tower`.

Considerações sobre design

- RCPs afetam somente os recursos nas contas dos membros da organização. Elas não têm efeito sobre os recursos na conta gerencial. Isso também significa que RCPs se aplicam às contas de membros designadas como administradores delegados.
- RCPs aplicam-se aos recursos de um subconjunto de. Serviços da AWS Para obter mais informações, consulte Lista Serviços da AWS desse suporte RCPs na AWS Organizations documentação. Você pode usar Regras do AWS ConfigAWS Lambdaas funções para monitorar e automatizar a aplicação de controles de segurança em recursos que atualmente não são suportados pelo RCPs.

Políticas declarativas

Uma política declarativa é um tipo de política de AWS Organizations gerenciamento que ajuda você a declarar e aplicar centralmente a configuração desejada para uma determinada escala AWS service (Serviço da AWS) em toda a organização. Atualmente, as políticas declarativas oferecem suporte aos serviços Amazon EC2, Amazon VPC e Amazon EBS. Os atributos de serviço disponíveis incluem aplicar o Instance Metadata Service Version 2 (IMDSv2), permitir a solução de problemas por meio do console serial EC2, permitir configurações de Amazon Machine Image (AMI) e bloquear o acesso público a snapshots do Amazon EBS, Amazon EC2 e recursos da Amazon VPC. AMIs Para obter os serviços e atributos suportados mais recentes, consulte Políticas declarativas na AWS Organizations documentação.

Você pode aplicar a configuração básica de um AWS service (Serviço da AWS) fazendo algumas seleções nos AWS Control Tower consoles AWS Organizations e ou usando alguns comandos AWS Command Line Interface (AWS CLI) e SDK. AWS As políticas declarativas são aplicadas no plano de controle do serviço, o que significa que a configuração básica de um AWS service (Serviço da AWS) é sempre mantida, mesmo quando o serviço introduz novos recursos ou APIs quando novas contas são adicionadas a uma organização ou quando novos diretores e recursos são criados. As políticas declarativas podem ser aplicadas a uma organização inteira ou a contas específicas OUs . A política efetiva é o conjunto de regras herdadas da raiz da organização e OUs junto com as políticas diretamente vinculadas à conta. Se uma política declarativa for desanexada, o estado do atributo voltará ao estado anterior à anexação da política declarativa.

Você pode usar políticas declarativas para criar mensagens de erro personalizadas. Por exemplo, se uma operação de API falhar devido a uma política declarativa, você pode definir a mensagem de erro ou fornecer um URL personalizado, como um link para um wiki interno ou um link para uma mensagem que descreva a falha. Isso ajuda a fornecer aos usuários mais informações para que eles mesmos possam solucionar o problema. Você também pode auditar o processo de criação de políticas declarativas, atualização de políticas declarativas e exclusão de políticas declarativas usando. AWS CloudTrail

As políticas declarativas fornecem relatórios de status da conta, que permitem que você revise o status atual de todos os atributos que são suportados pelas políticas declarativas das contas no escopo. Você pode escolher as contas e OUs incluí-las no escopo do relatório ou escolher uma organização inteira selecionando a raiz. Esse relatório ajuda você a avaliar a prontidão fornecendo um detalhamento Região da AWS e especificando se o estado atual de um atributo é uniforme em todas as contas (por meio do `numberOfMatchedAccounts` valor) ou inconsistente em todas as contas (por meio do `numberOfUnmatchedAccounts` valor).

> **Considerações sobre design**
>
> Quando você configura um atributo de serviço usando uma política declarativa, a política pode afetar vários APIs. Qualquer ação não compatível falhará. Os administradores da conta não poderão modificar o valor do atributo de serviço no nível da conta individual.

Acesso root centralizado

Todas as contas de membros AWS Organizations têm seu próprio usuário raiz, que é uma identidade que tem acesso completo a todos Serviços da AWS os recursos dessa conta de membro. O IAM

fornece gerenciamento centralizado de acesso raiz para gerenciar o acesso raiz em todas as contas dos membros. Isso ajuda a evitar o uso do usuário root como membro e ajuda a fornecer recuperação em grande escala. O recurso de acesso raiz centralizado tem dois recursos essenciais: gerenciamento de credenciais raiz e sessões raiz.

- O recurso de gerenciamento de credenciais raiz permite o gerenciamento central e ajuda a proteger o usuário raiz em todas as contas de gerenciamento. Esse recurso inclui a remoção de credenciais raiz de longo prazo, a prevenção da recuperação da credencial raiz por contas de membros e o provisionamento de novas contas de membros sem credenciais raiz por padrão. Ele também fornece uma maneira fácil de demonstrar conformidade. Quando o gerenciamento do usuário raiz é centralizado, você pode remover senhas do usuário raiz, chaves de acesso e certificados de assinatura, além de desativar a autenticação multifator (MFA) de todas as contas dos membros.
- O recurso de sessões raiz permite que você execute ações privilegiadas de usuário raiz usando credenciais de curto prazo em contas de membros da conta de gerenciamento da organização ou de contas de administrador delegado. Esse recurso ajuda você a habilitar o acesso raiz de curto prazo que tenha como escopo ações específicas, aderindo ao princípio do privilégio mínimo.

Para o gerenciamento centralizado de credenciais raiz, você precisa habilitar os recursos de gerenciamento de credenciais raiz e sessões raiz no nível da organização a partir da conta de gerenciamento da organização ou em uma conta de administrador delegado. Seguindo as melhores práticas da AWS SRA, delegamos esse recurso à conta do Security Tooling. Para obter informações sobre como configurar e usar o acesso centralizado do usuário raiz, consulte a postagem do blog AWS de segurança, Gerenciamento centralizado do acesso raiz para clientes que usam. AWS Organizations

Centro de Identidade do IAM

Centro de Identidade do AWS IAMé um serviço de federação de identidades que ajuda você a gerenciar centralmente o acesso por SSO a todas as suas cargas de Contas da AWS trabalho, principais e na nuvem. O IAM Identity Center também ajuda você a gerenciar o acesso e as permissões aos aplicativos de software como serviço (SaaS) de terceiros comumente usados. Os provedores de identidade se integram ao IAM Identity Center usando o SAML 2.0. O just-in-time provisionamento em massa pode ser feito usando o System for Cross-Domain Identity Management (SCIM). O IAM Identity Center também pode se integrar a domínios locais ou AWS gerenciados do Microsoft Active Directory (AD) como um provedor de identidade por meio do uso de. AWS

Directory Service O IAM Identity Center inclui um portal de usuário onde seus usuários finais podem encontrar e acessar o Contas da AWS IAM Identity Center, as funções, os aplicativos em nuvem e os aplicativos personalizados atribuídos em um só lugar.

O IAM Identity Center se integra de forma nativa AWS Organizations e é executado na conta de gerenciamento da organização por padrão. No entanto, para exercer o mínimo de privilégios e controlar rigorosamente o acesso à conta de gerenciamento, a administração do IAM Identity Center pode ser delegada a uma conta de membro específica. No AWS SRA, a conta do Shared Services é a conta de administrador delegado do IAM Identity Center. Antes de habilitar a administração delegada para o IAM Identity Center, analise essas considerações. Você encontrará mais informações sobre delegação na seção Conta do Shared Services. Mesmo depois de habilitar a delegação, o IAM Identity Center ainda precisa ser executado na conta de gerenciamento da organização para realizar determinadas tarefas relacionadas ao IAM Identity Center, que incluem o gerenciamento de conjuntos de permissões provisionados na conta de gerenciamento da organização.

No console do IAM Identity Center, as contas são exibidas por sua OU encapsuladora. Isso permite que você descubra rapidamente suas permissões Contas da AWS, aplique conjuntos comuns de permissões e gerencie o acesso a partir de um local central.

O IAM Identity Center inclui um repositório de identidades onde informações específicas do usuário devem ser armazenadas. No entanto, o IAM Identity Center não precisa ser a fonte autorizada de informações da força de trabalho. Nos casos em que sua empresa já tem uma fonte autorizada, o IAM Identity Center oferece suporte aos seguintes tipos de provedores de identidade ()IdPs.

- Armazenamento de identidades do IAM Identity Center — Escolha essa opção se as duas opções a seguir não estiverem disponíveis. Os usuários são criados, as atribuições de grupos são feitas e as permissões são atribuídas no repositório de identidades. Mesmo que sua fonte autorizada seja externa ao IAM Identity Center, uma cópia dos atributos principais será armazenada no repositório de identidades.
- Microsoft Active Directory (AD) — Escolha essa opção se quiser continuar gerenciando usuários em seu diretório AWS Directory Service for Microsoft Active Directory ou em seu diretório autogerenciado no Active Directory.
- Provedor de identidade externo — Escolha essa opção se você preferir gerenciar usuários em um IdP externo de terceiros baseado em SAML.

Você pode confiar em um IdP existente que já esteja em vigor na sua empresa. Isso facilita o gerenciamento do acesso em várias aplicações e sistemas, pois você está criando, gerenciando e revogando o acesso de um único local. Por exemplo, se alguém deixar sua equipe, você poderá revogar o acesso dessa pessoa a todos os aplicativos e serviços (inclusive Contas da AWS) em um único local. Isso reduz a necessidade de várias credenciais e oferece a oportunidade de integração com seus processos de recursos humanos (RH).

> Considerações sobre design
>
> Use um IdP externo se essa opção estiver disponível para sua empresa. Se o seu IdP for compatível com o System for Cross-domain Identity Management (SCIM), aproveite o recurso SCIM no IAM Identity Center para automatizar o provisionamento (sincronização) de usuários, grupos e permissões. Isso permite que o AWS acesso permaneça sincronizado com seu fluxo de trabalho corporativo para novos contratados, funcionários que estão mudando para outra equipe e funcionários que estão deixando a empresa. A qualquer momento, você pode ter somente um diretório ou um provedor de identidade SAML 2.0 conectado ao IAM Identity Center. No entanto, você pode mudar para outro provedor de identidade.

Consultor de acesso IAM

O consultor de acesso do IAM fornece dados de rastreabilidade na forma de informações do último acesso do serviço para você e. Contas da AWS OUs Use esse controle de detetive para contribuir com uma estratégia de privilégios mínimos. Para diretores do IAM, você pode visualizar dois tipos de informações do último acesso: informações permitidas e AWS service (Serviço da AWS) informações sobre ações permitidas. As informações incluem a data e a hora em que a tentativa foi feita.

O acesso ao IAM na conta de gerenciamento da organização permite que você visualize os dados do último acesso do serviço para a conta de gerenciamento da organização, a OU, a conta do membro ou a política do IAM em sua AWS organização. Essas informações estão disponíveis no console do IAM dentro da conta de gerenciamento e também podem ser obtidas de forma programática usando o consultor APIs de acesso do IAM AWS CLI ou um cliente programático. As informações indicam quais entidades principais de uma organização ou conta tentaram acessar o serviço pela última vez e quando. As informações do último acesso fornecem informações sobre o uso real do serviço (veja exemplos de cenários), para que você possa reduzir as permissões do IAM somente para os serviços que são realmente usados.

AWS Systems Manager

O Quick Setup e o Explorer, que são recursos do AWS Systems Manager, oferecem suporte AWS Organizations e operam a partir da conta de gerenciamento da organização.

O Quick Setup é um recurso de automação do Systems Manager. Ele permite que a conta de gerenciamento da organização defina facilmente as configurações para que o Systems Manager interaja em seu nome em todas as contas AWS da sua organização. Você pode ativar a Configuração rápida em toda a AWS organização ou escolher uma opção específica OUs. O Quick Setup pode programar o AWS Systems Manager Agente (Agente SSM) para executar atualizações quinzenais em suas instâncias do EC2 e pode configurar uma verificação diária dessas instâncias para identificar os patches ausentes.

O Explorer é um painel de operações personalizável que relata informações sobre seus AWS recursos. O Explorer exibe uma visão agregada dos dados operacionais de suas AWS contas e de todas Regiões da AWS as partes. Isso inclui dados sobre suas instâncias do EC2 e detalhes de conformidade de patches. Depois de concluir a Configuração Integrada (que também inclui o Systems Manager OpsCenter) AWS Organizations, você pode agregar dados no Explorer por OU ou para uma AWS organização inteira. O Systems Manager agrega os dados na conta de gerenciamento da AWS organização antes de exibi-los no Explorer.

A seção Workloads OU, mais adiante neste guia, discute o uso do SSM Agent nas instâncias do EC2 na conta do aplicativo.

AWS Control Tower

AWS Control Towerfornece uma maneira simples de configurar e controlar um AWS ambiente seguro com várias contas, chamado de landing zone. AWS Control Tower cria sua landing zone usando AWS Organizations e fornece gerenciamento e governança contínuos de contas, bem como as melhores práticas de implementação. Você pode usar AWS Control Tower para provisionar novas contas em algumas etapas e, ao mesmo tempo, garantir que as contas estejam em conformidade com suas políticas organizacionais. Você pode até mesmo adicionar contas existentes a um novo AWS Control Tower ambiente.

AWS Control Tower tem um conjunto amplo e flexível de recursos. Um recurso importante é a capacidade de orquestrar os recursos de vários outros Serviços da AWS AWS Organizations AWS Service Catalog, incluindo o IAM Identity Center, para criar uma landing zone. Por exemplo, por padrão, AWS Control Tower usa AWS CloudFormation para estabelecer uma linha de base, políticas

AWS Organizations de controle de serviço (SCPs) para evitar alterações na configuração e Regras do AWS Config regras para detectar continuamente a não conformidade. AWS Control Tower emprega esquemas que ajudam você a alinhar rapidamente seu AWS ambiente de várias contas aos princípios de design da base de segurança da AWS Well Architected. Entre os recursos de governança, AWS Control Tower oferece proteções que impedem a implantação de recursos que não estão em conformidade com as políticas selecionadas.

Você pode começar a implementar a orientação AWS da SRA com AWS Control Tower. Por exemplo, AWS Control Tower estabelece uma AWS organização com a arquitetura de várias contas recomendada. Ele fornece planos para fornecer gerenciamento de identidade, fornecer acesso federado às contas, centralizar o registro, estabelecer auditorias de segurança entre contas, definir um fluxo de trabalho para provisionar novas contas e implementar linhas de base de contas com configurações de rede.

No AWS SRA, AWS Control Tower está dentro da conta de gerenciamento da organização porque AWS Control Tower usa essa conta para configurar uma AWS organização automaticamente e designa essa conta como a conta de gerenciamento. Essa conta é usada para cobrança em toda a sua AWS organização. Também é usado para o provisionamento de contas do Account Factory, para gerenciar OUs e gerenciar grades de proteção. Se você estiver lançando AWS Control Tower em uma AWS organização existente, poderá usar a conta de gerenciamento existente. AWS Control Tower usará essa conta como a conta de gerenciamento designada.

> **Considerações sobre design**
>
> Se você quiser criar uma linha de base adicional de controles e configurações em suas contas, você pode usar Personalizações para (cFct). AWS Control Tower Com o CFct, você pode personalizar sua AWS Control Tower landing zone usando um CloudFormation modelo e. SCPs Você pode implantar o modelo e as políticas personalizados em contas individuais e OUs dentro da sua organização. O cFct se integra aos eventos AWS Control Tower do ciclo de vida para garantir que as implantações de recursos permaneçam sincronizadas com sua landing zone.

AWS Artifact

AWS Artifactfornece acesso sob demanda a relatórios AWS de segurança e conformidade e a contratos on-line selecionados. Os relatórios disponíveis em AWS Artifact incluem relatórios de

Controles Organizacionais e de Sistema (SOC), relatórios do Setor de Cartões de Pagamento (PCI) e certificações de órgãos de credenciamento de várias regiões e setores de conformidade que validam a implementação e a eficácia operacional dos controles de segurança. AWS AWS Artifact ajuda você a realizar sua devida diligência AWS com maior transparência em nosso ambiente de controle de segurança. Também permite monitorar continuamente a segurança e a conformidade AWS com o acesso imediato a novos relatórios.

AWS Artifact Os contratos permitem que você revise, aceite e acompanhe o status de AWS contratos, como o Adendo de Associado Comercial (BAA) para uma conta individual e para as contas que fazem parte da sua organização. AWS Organizations

Você pode fornecer os artefatos de AWS auditoria aos seus auditores ou reguladores como evidência dos controles de AWS segurança. Você também pode usar a orientação de responsabilidade fornecida por alguns dos artefatos de AWS auditoria para projetar sua arquitetura de nuvem. Essa orientação ajuda a determinar os controles de segurança adicionais que você pode implementar para dar suporte aos casos de uso específicos do seu sistema.

AWS Artifact é hospedado na conta de gerenciamento da organização para fornecer um local central onde você pode revisar, aceitar e gerenciar contratos com AWS. Isso ocorre porque os contratos que são aceitos na conta de gerenciamento fluem para as contas dos membros.

> **Considerações sobre design**
>
> Os usuários da conta de gerenciamento da organização devem ser restritos a usar somente o recurso Acordos AWS Artifact e nada mais. Para implementar a segregação de funções, também AWS Artifact está hospedado na conta do Security Tooling, onde você pode delegar permissões às partes interessadas em conformidade e aos auditores externos para acessar artefatos de auditoria. Você pode implementar essa separação definindo políticas refinadas de permissão do IAM. Para ver exemplos, consulte Exemplos de políticas do IAM na AWS documentação.

Guardrails de serviços de segurança distribuídos e centralizados

No AWS SRA,,, Amazon AWS Security Hub AWS Security Hub CSPM, IAM Access Analyzer GuardDuty AWS Config, as trilhas AWS CloudTrail da organização e, frequentemente, o Amazon Macie são implantadas com um conjunto delegado apropriado de proteções em todas as contas e também fornecem monitoramento, gerenciamento e governança centralizados em toda a

organização. AWS Você encontrará esse grupo de serviços em cada tipo de conta representada na AWS SRA. Eles devem fazer parte do Serviços da AWS que deve ser provisionado como parte do processo de integração e definição de linha de base da sua conta. O repositório de GitHub código fornece um exemplo de implementação de serviços AWS focados na segurança em suas contas, incluindo a conta de gerenciamento da organização. AWS

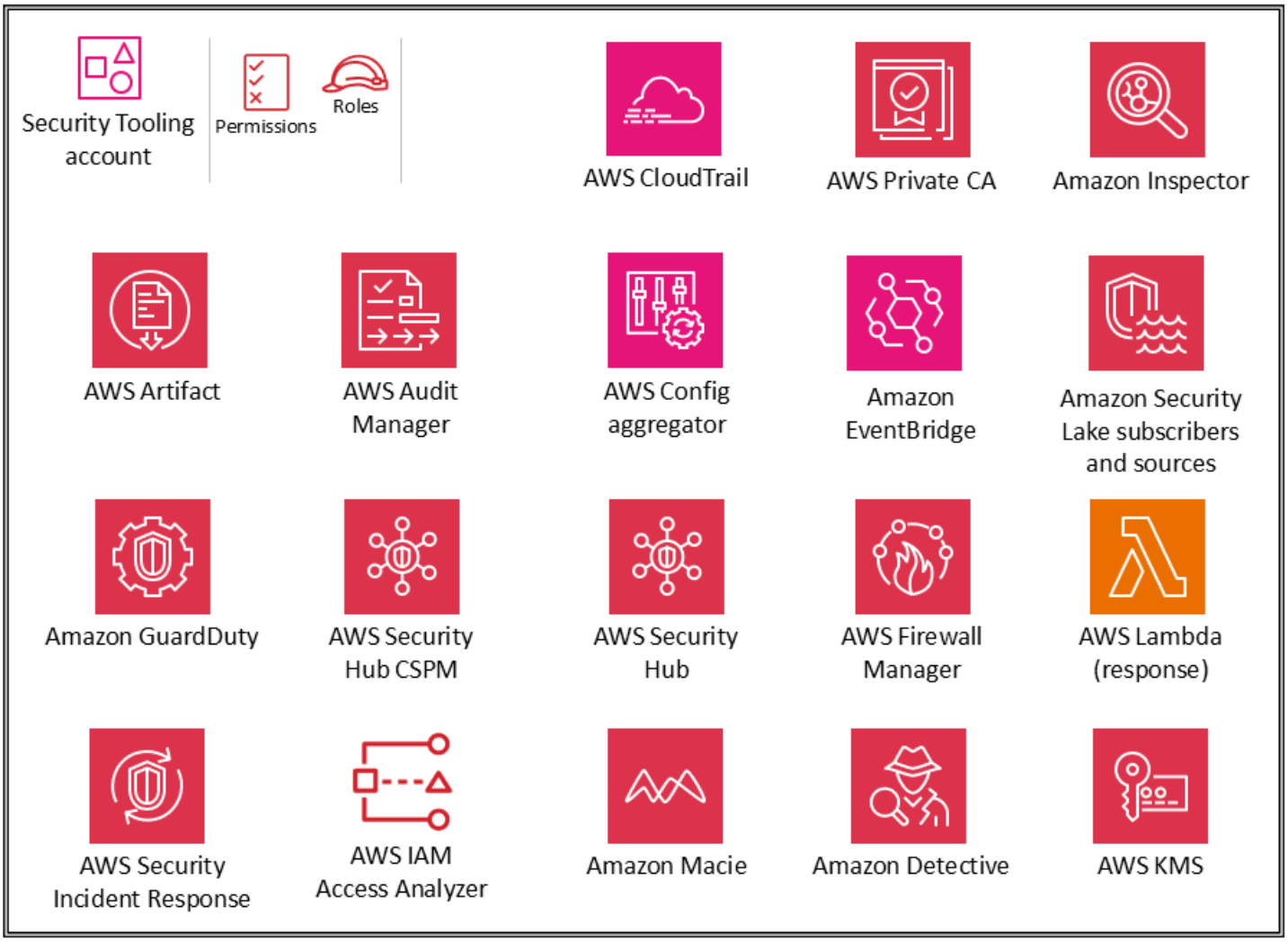
Além desses serviços, o AWS SRA inclui dois serviços focados em segurança, Amazon Detective e, que oferecem suporte à integração AWS Audit Manager e à funcionalidade de administrador delegado no. AWS Organizations No entanto, eles não estão incluídos como parte dos serviços recomendados para a definição de base da conta. Vimos que esses serviços são melhor usados nos seguintes cenários:

- Você tem uma equipe dedicada ou um grupo de recursos que executam essas funções forenses digitais e de auditoria de TI. O Detective é melhor utilizado pelas equipes de analistas de segurança, e o Audit Manager é útil para suas equipes internas de auditoria ou conformidade.
- Você quer se concentrar em um conjunto básico de ferramentas AWS Config, como Amazon e GuardDuty AWS Security Hub, AWS Security Hub CSPM no início do seu projeto, e depois desenvolvê-las usando serviços que fornecem recursos adicionais.

UO de segurança | Conta do Security Tooling

> Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços AWS de segurança que estão configurados na conta do Security Tooling.



A conta do Security Tooling é dedicada a operar serviços de segurança Contas da AWS, monitorar e automatizar alertas e respostas de segurança. Os objetivos de segurança incluem o seguinte:

- Forneça uma conta dedicada com acesso controlado para gerenciar o acesso às barreiras de segurança, monitoramento e resposta.
- Mantenha a infraestrutura de segurança centralizada apropriada para monitorar os dados das operações de segurança e manter a rastreabilidade. Detecção, investigação e resposta são partes essenciais do ciclo de vida da segurança e podem ser usadas para apoiar um processo de qualidade, uma obrigação legal ou de conformidade e para esforços de identificação e resposta a ameaças.
- Apoie ainda mais a estratégia defense-in-depth da organização mantendo outra camada de controle sobre a configuração e as operações de segurança apropriadas, como chaves de criptografia e configurações de grupos de segurança. Essa é uma conta na qual os operadores

de segurança trabalham. As funções somente de leitura/auditoria para visualizar informações de AWS toda a organização são típicas, enquanto as write/modify funções são limitadas em número, rigorosamente controladas, monitoradas e registradas.

Considerações sobre design

- AWS Control Tower nomeia a conta na OU de segurança como Conta de Auditoria por padrão. Você pode renomear a conta durante a AWS Control Tower configuração.
- Talvez seja apropriado ter mais de uma conta do Security Tooling. Por exemplo, o monitoramento e a resposta a eventos de segurança geralmente são atribuídos a uma equipe dedicada. A segurança da rede pode garantir sua própria conta e funções em colaboração com a infraestrutura de nuvem ou a equipe de rede. Essas divisões mantêm o objetivo de separar os enclaves de segurança centralizados e enfatizam ainda mais a separação de tarefas, privilégios mínimos e a simplicidade potencial das atribuições da equipe. Se você estiver usando AWS Control Tower, isso restringe a criação de adicionais na Contas da AWS OU de segurança.

Administrador delegado para serviços de segurança

A conta do Security Tooling serve como conta de administrador para serviços de segurança que são gerenciados em uma administrator/member estrutura em todo o. Contas da AWS Conforme mencionado anteriormente, isso é feito por meio da funcionalidade de administrador AWS Organizations delegado. Os serviços no AWS SRA que atualmente oferecem suporte ao administrador delegado incluem o gerenciamento centralizado de acesso root pelo IAM,, AWS Firewall Manager Amazon AWS Config, IAM Access Analyzer GuardDuty, Amazon Macie,,, Amazon Detective AWS Security Hub,, AWS Security Hub CSPM Amazon Inspector, AWS Audit Manager, e. AWS CloudTrail AWS Systems Manager Sua equipe de segurança gerencia os recursos de segurança desses serviços e monitora quaisquer eventos ou descobertas específicos de segurança.

Centro de Identidade do AWS IAM oferece suporte à administração delegada a uma conta de membro. AWS A SRA usa a conta do Shared Services como a conta de administrador delegado para o IAM Identity Center, conforme explicado posteriormente na seção IAM Identity Center da conta do Shared Services.

Acesso root centralizado

A conta do Security Tooling é a conta de administrador delegado para o gerenciamento centralizado da capacidade de acesso raiz do IAM. Esse recurso deve ser ativado no nível da organização, permitindo o gerenciamento de credenciais e a ação raiz privilegiada nas contas dos membros. Os administradores delegados precisam receber `sts:AssumeRoot` permissões explícitas para poderem realizar ações raiz privilegiadas em nome das contas dos membros. Essa permissão está disponível somente depois que a ação raiz privilegiada em uma conta de membro é ativada no Gerenciamento da organização ou na conta de administrador delegado. Com essa permissão, os usuários podem realizar tarefas privilegiadas de usuário root nas contas dos membros, centralmente a partir da conta do Security Tooling. Depois de iniciar uma sessão privilegiada, você pode excluir uma política de bucket do S3 mal configurada, excluir uma política de fila SQS mal configurada, excluir as credenciais do usuário raiz de uma conta membro e reativar as credenciais do usuário raiz para uma conta membro. Você pode realizar essas ações no console, usando o AWS Command Line Interface (AWS CLI) ou por meio de APIs.

AWS CloudTrail

AWS CloudTrailé um serviço que oferece suporte à governança, conformidade e auditoria das atividades em seu Conta da AWS. Com CloudTrail, você pode registrar, monitorar continuamente e reter as atividades da conta relacionadas às ações em toda a sua AWS infraestrutura. CloudTrail está integrado com AWS Organizations, e essa integração pode ser usada para criar uma única trilha que registra todos os eventos de todas as contas na AWS organização. Elas são chamadas de trilhas da organização. Você pode criar e gerenciar uma trilha da organização somente de dentro da conta de gerenciamento da organização ou de uma conta de administrador delegado. Quando você cria uma trilha da organização, uma trilha com o nome que você especifica é criada em todas as Conta da AWS que pertencem à sua AWS organização. A trilha registra a atividade de todas as contas, incluindo a conta de gerenciamento, na AWS organização e armazena os registros em um único bucket do S3. Devido à sensibilidade desse bucket do S3, você deve protegê-lo seguindo as melhores práticas descritas na seção Amazon S3 como armazenamento de log central, mais adiante neste guia. Todas as contas da AWS organização podem ver a trilha da organização em sua lista de trilhas. No entanto, os membros Contas da AWS têm acesso somente para visualização a essa trilha. Por padrão, quando você cria uma trilha da organização no CloudTrail console, a trilha é uma trilha multirregional. Para obter mais práticas recomendadas de segurança, consulte a CloudTraildocumentação.

No AWS SRA, a conta do Security Tooling é a conta de administrador delegado para gerenciamento. CloudTrail O bucket do S3 correspondente para armazenar os registros de trilhas da organização é criado na conta do Log Archive. Isso serve para separar o gerenciamento e o uso dos privilégios de CloudTrail log. Para obter informações sobre como criar ou atualizar um bucket do S3 para armazenar arquivos de log para uma trilha organizacional, consulte a CloudTrail documentação. Como prática recomendada de segurança, adicione a chave de `aws:SourceArn` condição da trilha da organização à política de recursos do bucket do S3 (e a quaisquer outros recursos, como chaves KMS ou tópicos do SNS). Isso garante que o bucket do S3 aceite somente dados associados à trilha específica. A trilha é configurada com a validação do arquivo de log para validação da integridade do arquivo de log. Os arquivos de log e resumo são criptografados usando o SSE-KMS. A trilha da organização também é integrada a um grupo de CloudWatch registros no Logs para enviar eventos para retenção de longo prazo.

Note

Você pode criar e gerenciar trilhas organizacionais a partir das contas de gerenciamento e de administrador delegado. No entanto, como prática recomendada, você deve limitar o acesso à conta de gerenciamento e usar a funcionalidade de administrador delegado onde ela estiver disponível.

Considerações sobre design

- CloudTrail não registra eventos de dados por padrão, porque geralmente são atividades de alto volume. No entanto, você deve capturar eventos de dados para AWS recursos críticos específicos, como buckets S3, funções Lambda, eventos de log externos AWS que são enviados para o CloudTrail lago e tópicos do SNS. Para fazer isso, configure a trilha da sua organização para incluir eventos de dados ARNs de recursos específicos especificando cada recurso individual.
- Se uma conta membro exigir acesso aos arquivos de CloudTrail log de sua própria conta, você poderá compartilhar seletivamente os arquivos de CloudTrail log da organização a partir do bucket central do S3. No entanto, se as contas membros exigirem grupos de CloudWatch registros locais da Amazon para CloudTrail os registros de suas contas ou quiserem configurar o gerenciamento de registros e os eventos de dados (somente leitura, somente gravação, eventos de gerenciamento, eventos de dados) de forma diferente da

trilha da organização, elas poderão criar uma trilha local com os controles apropriados. As trilhas específicas da conta local têm um custo adicional.

AWS Security Hub CSPM

AWS Security Hub O Cloud Security Posture Management (AWS Security Hub CSPM), anteriormente conhecido como AWS Security Hub, fornece uma visão abrangente de sua postura de segurança AWS e ajuda você a verificar seu ambiente em relação aos padrões e melhores práticas do setor de segurança. O Security Hub CSPM coleta dados de segurança de vários serviços AWS integrados, produtos de terceiros compatíveis e outros produtos de segurança personalizados que você possa usar. O Security Hub facilita a análise das tendências de segurança e a identificação dos problemas de segurança de maior prioridade. Além das fontes ingeridas, o Security Hub CSPM gera suas próprias descobertas, que são representadas por controles de segurança mapeados para um ou mais padrões de segurança. Esses padrões incluem AWS Foundational Security Best Practices (FSBP), Center for Internet Security (CIS) AWS Foundations Benchmark v1.20 e v1.4.0, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5, Payment Card Industry Data Security Standard (PCI DSS) e padrões gerenciados por serviços. Para obter uma lista dos padrões de segurança atuais e detalhes sobre controles de segurança específicos, consulte a referência de padrões para o CSPM do Security Hub na documentação do CSPM do Security Hub.

O Security Hub CSPM se integra AWS Organizations para simplificar o gerenciamento da postura de segurança em todas as suas contas existentes e futuras em sua organização. AWS Você pode usar o recurso de configuração central do Security Hub CSPM da conta do administrador delegado (nesse caso, o Security Tooling) para especificar como o serviço CSPM, os padrões de segurança e os controles de segurança do Security Hub são configurados nas contas e unidades organizacionais () da sua organização em todas as regiões. OUs Você pode definir essas configurações em algumas etapas a partir de uma região primária, chamada de região de origem. Se você não usa a configuração central, deve configurar o CSPM do Security Hub separadamente em cada conta e região. O administrador delegado pode designar contas e OUs como autogerenciadas, onde o membro pode definir as configurações separadamente em cada região, ou como gerenciadas centralmente, onde o administrador delegado pode configurar a conta do membro ou a OU em todas as regiões. Você pode designar todas as contas e OUs em sua organização como gerenciadas centralmente, todas autogerenciadas ou uma combinação de ambas. Isso simplifica a aplicação de uma configuração consistente e, ao mesmo tempo, fornece a flexibilidade de modificá-la para cada UO e conta.

A conta de administrador delegado do Security Hub CSPM também pode visualizar descobertas, ver insights e detalhes de controle de todas as contas dos membros. Além disso, você pode designar uma região de agregação na conta do administrador delegado para centralizar suas descobertas em suas contas e regiões vinculadas. Suas descobertas são sincronizadas de forma contínua e bidirecional entre a região agregadora e todas as outras regiões.

O Security Hub CSPM suporta integrações com vários. Serviços da AWS A Amazon GuardDuty AWS Config, o Amazon Macie, o IAM Access Analyzer, o Amazon AWS Firewall Manager Inspector, o Amazon Route 53 Resolver DNS Firewall e o AWS Systems Manager Patch Manager podem alimentar as descobertas para o CSPM do Security Hub. O Security Hub CSPM processa as descobertas usando um formato padrão chamado AWS Security Finding Format (ASFF). O Security Hub CSPM correlaciona as descobertas em produtos integrados para priorizar os mais importantes. Você pode enriquecer os metadados das descobertas do CSPM do Security Hub para ajudar a contextualizar, priorizar e agir melhor com base nas descobertas de segurança. Esse enriquecimento adiciona tags de recursos, uma nova tag de AWS aplicativo e informações do nome da conta a cada descoberta que é ingerida no CSPM do Security Hub. Isso ajuda você a ajustar as descobertas das regras de automação, pesquisar ou filtrar descobertas e insights e avaliar o status da postura de segurança por aplicativo. Além disso, você pode usar regras de automação para atualizar automaticamente as descobertas. À medida que o Security Hub CSPM ingere as descobertas, ele pode aplicar uma variedade de ações de regras, como suprimir descobertas, alterar sua gravidade e adicionar notas às descobertas. Essas ações de regra entram em vigor quando as descobertas correspondem aos critérios especificados, como o recurso ou IDs a conta à qual a descoberta está associada ou seu título. Você pode usar regras de automação para atualizar campos de busca selecionados no ASFF. As regras se aplicam tanto às descobertas novas quanto às atualizadas.

Durante a investigação de um evento de segurança, você pode navegar do Security Hub CSPM até o Amazon Detective para investigar uma descoberta. GuardDuty O Security Hub CSPM recomenda alinhar as contas de administrador delegado para serviços como Detective (onde elas existem) para uma integração mais suave. Por exemplo, se você não alinhar as contas de administrador entre o Detective e o CSPM do Security Hub, a navegação das descobertas para o Detective não funcionará. Para obter uma lista abrangente, consulte Visão geral das AWS service (Serviço da AWS) integrações com o CSPM do Security Hub na documentação do CSPM do Security Hub.

Você pode usar o Security Hub CSPM com o recurso Network Access Analyzer da Amazon VPC para ajudar a monitorar continuamente a conformidade da sua configuração de rede. AWS Isso ajudará você a bloquear o acesso indesejado à rede e a impedir que seus recursos essenciais tenham acesso externo. Para obter mais detalhes sobre arquitetura e implementação, consulte

a postagem do AWS blog Verificação contínua da conformidade da rede usando o Amazon VPC Network Access Analyzer e. AWS Security Hub CSPM

Além de seus recursos de monitoramento, o Security Hub CSPM oferece suporte à integração com EventBridge a Amazon para automatizar a correção de descobertas específicas. Você pode definir ações personalizadas a serem tomadas quando uma descoberta for recebida. Por exemplo, é possível configurar ações personalizadas para enviar as descobertas a um sistema de criação de tíquetes ou a um sistema automatizado de correção. Para discussões e exemplos adicionais, consulte as postagens do AWS blog Resposta e remediação automatizadas com AWS Security Hub CSPM e Como implantar a AWS solução para resposta e remediação automatizadas do Security Hub CSPM.

O Security Hub CSPM usa serviços vinculados Regras do AWS Config para realizar a maioria de suas verificações de segurança para controles. Para oferecer suporte a esses controles, AWS Config devem estar habilitados em todas as contas, incluindo a conta do administrador (ou administrador delegado) e as contas dos membros, em cada uma em que o CSPM do Security Região da AWS Hub esteja habilitado.

Considerações sobre design

- Se um padrão de conformidade, como o PCI-DSS, já estiver presente no CSPM do Security Hub, o serviço CSPM do Security Hub totalmente gerenciado é a maneira mais fácil de operacionalizá-lo. No entanto, se você quiser montar seu próprio padrão de conformidade ou segurança, que pode incluir verificações de segurança, operacionais ou de otimização de custos, os pacotes de AWS Config conformidade oferecem um processo de personalização simplificado. (Para obter mais informações AWS Config e pacotes de conformidade, consulte a AWS Configseção.)
- Os casos de uso comuns do Security Hub CSPM incluem o seguinte:
  - Como um painel que fornece visibilidade aos proprietários de aplicativos sobre a postura de segurança e conformidade de seus recursos AWS
  - Como uma visão central das descobertas de segurança usadas por operações de segurança, agentes de resposta a incidentes e caçadores de ameaças para fazer a triagem e tomar medidas sobre as descobertas de AWS segurança e conformidade em todas as regiões Contas da AWS

- Para agregar e encaminhar descobertas de segurança e conformidade de todas Contas da AWS as regiões para um gerenciamento centralizado de informações e eventos de segurança (SIEM) ou outro sistema de orquestração de segurança

Para obter orientações adicionais sobre esses casos de uso, incluindo como configurá-los, consulte a postagem do blog Três padrões de uso recorrentes do CSPM do Security Hub e como implantá-los.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação do CSPM do Security Hub. Inclui ativação automática do serviço, administração delegada a uma conta membro (Security Tooling) e configuração para habilitar o CSPM do Security Hub para todas as contas existentes e futuras na organização. AWS

AWS Security Hub

AWS Security Hubé uma solução unificada de segurança em nuvem que prioriza suas ameaças críticas à segurança e ajuda você a responder em grande escala. O Security Hub detecta problemas de segurança quase em tempo real correlacionando e enriquecendo automaticamente sinais de segurança de várias fontes, como gerenciamento de postura (AWS Security Hub CSPM), gerenciamento de vulnerabilidades (Amazon Inspector), dados confidenciais (Amazon Macie) e detecção de ameaças (Amazon). GuardDuty Isso permite que as equipes de segurança priorizem os riscos ativos em seus ambientes de nuvem por meio de análises automatizadas e insights contextuais. O Security Hub fornece uma representação visual do possível caminho de ataque que os invasores podem explorar para obter acesso aos recursos associados a uma descoberta de exposição. Isso transforma sinais de segurança complexos em insights acionáveis, para que você possa tomar decisões informadas sobre sua segurança rapidamente.

O Security Hub foi estrategicamente redesenhado para simplificar a habilitação dos componentes do serviço de segurança associado para chegar a um resultado de segurança. Ao correlacionar as descobertas de segurança em uma matriz de ameaças em diferentes sinais de segurança quase em tempo real, você pode priorizar primeiro os riscos mais críticos. As descobertas são correlacionadas para detectar a exposição associada aos AWS recursos. As exposições representam fraquezas mais amplas nos controles de segurança, configurações incorretas ou outras áreas que poderiam

ser exploradas por ameaças ativas. Por exemplo, uma exposição pode ser uma instância do EC2 que pode ser acessada pela Internet e tem vulnerabilidades de software com alta probabilidade de exploração.

O Security Hub e o Security Hub CSPM são serviços complementares. O Security Hub CSPM fornece uma visão abrangente de sua postura de segurança e ajuda você a avaliar seu ambiente de nuvem em relação aos padrões e melhores práticas do setor de segurança. O Security Hub fornece uma experiência unificada que ajuda você a priorizar e responder a problemas críticos de segurança. As descobertas do CSPM do Security Hub são encaminhadas automaticamente para o Security Hub, onde são correlacionadas com as descobertas de outros serviços de segurança, como o Amazon Inspector, para gerar exposições. Isso ajuda você a identificar os riscos mais críticos em seu ambiente.

O Security Hub também fornece um resumo dos recursos em seu AWS ambiente por tipo e descobertas associadas. Os recursos são priorizados por exposições e sequências de ataque. Ao escolher um tipo de recurso, você pode revisar todos os recursos associados a esse tipo de recurso.

Para uma experiência ideal, recomendamos habilitar o Security Hub e o Security Hub CSPM, bem como habilitar esses outros serviços de segurança: Amazon GuardDuty, AmazonInspector e Amazon Macie. Você pode ver se esses serviços e recursos estão uniformemente ativados em todas as contas dos membros da sua organização usando as descobertas da Cobertura do Security Hub.

No AWS SRA, a conta do Security Tooling atua como administrador delegado do Security Hub, do Security Hub CSPM e de outros serviços de segurança. AWS Na conta do Security Tooling, você pode ver todos os recursos associados às contas dos membros. Você também pode ver todos os recursos em sua casa Região da AWS no link Regiões da AWS.

> **Nota de implementação**
>
> A ativação do Security Hub requer três etapas, incluindo procedimentos que levam em consideração se você já habilitou o CSPM do Security Hub. O Security Hub é nativamente integrado ao AWS Organizations, o que simplifica o processo de configuração e implementação, além de centralizar e agregar todas as descobertas em um único local. De acordo com as melhores práticas do AWS SRA, use a conta do Security Tooling como a conta de administrador delegado para gerenciar e configurar o Security Hub. Use as configurações do Security Hub para habilitar todas as regiões e contas automaticamente, incluindo futuras regiões e contas. OUs Você também deve configurar a agregação entre regiões para agregar descobertas, recursos e tendências de várias Regiões da AWS em

uma única região de origem. Durante a configuração, você também pode ativar qualquer integração nativa, como o Jira Cloud ou. ServiceNow

Considerações sobre design

- As descobertas do Security Hub são formatadas no Open Cybersecurity Schema Framework (OCSF). O Security Hub gera descobertas no OCSF e recebe descobertas no OCSF do Security Hub CSPM e outros. Serviços da AWS Essas descobertas do OCSF podem ser enviadas EventBridge pela Amazon para automações ou armazenadas em uma conta central de agregação de registros para realizar análise e retenção de registros de segurança.
- A conta de gerenciamento da AWS organização não pode se designar como administrador delegado no Security Hub. Isso se alinha à prática recomendada da AWS SRA de designar a conta do Security Tooling como administrador delegado. Observe também:
  - A conta de administrador designada para o Security Hub CSPM se torna automaticamente o administrador designado para o Security Hub.
  - A remoção da administração delegada por meio do Security Hub também remove a administração delegada do CSPM do Security Hub. Da mesma forma, remover a administração delegada por meio do CSPM do Security Hub também a remove do Security Hub.
- O Security Hub inclui recursos que modificam e agem automaticamente com base nas descobertas com base em suas especificações. O Security Hub oferece suporte aos seguintes tipos de automações:
  - Regras de automação, que atualizam automaticamente as descobertas, suprimem as descobertas e enviam as descobertas para ferramentas de emissão de tíquetes quase em tempo real, com base em critérios definidos.
  - Resposta e remediação automatizadas, que criam EventBridge regras personalizadas que definem ações automáticas a serem tomadas em relação a descobertas e insights específicos.
- O Security Hub pode configurar o Amazon Inspector em todas as contas e regiões membros por meio de políticas, e pode configurar GuardDuty o CSPM do Security Hub por meio da implantação. As políticas geram AWS Organizations políticas para contas e regiões. As implantações são ações únicas que permitem um recurso de segurança em

contas e regiões selecionadas. As implantações não se aplicam às contas recém-ativadas. Como alternativa, você pode ativar automaticamente os recursos para novas contas de membros no GuardDuty Security Hub CSPM.

Amazon GuardDuty

GuardDutyA Amazon é um serviço de detecção de ameaças que monitora continuamente atividades maliciosas e comportamentos não autorizados para proteger você Contas da AWS e suas cargas de trabalho. Você deve sempre capturar e armazenar os registros apropriados para fins de monitoramento e auditoria, mas GuardDuty extrai fluxos independentes de dados diretamente dos registros de fluxo da AWS CloudTrail Amazon VPC e dos registros de DNS. AWS Você não precisa gerenciar as políticas de bucket do Amazon S3 nem modificar a forma como coleta e armazena seus registros. GuardDutyas permissões são gerenciadas como funções vinculadas a serviços que você pode revogar a qualquer momento desativando. GuardDuty Isso facilita a ativação do serviço sem configurações complexas e elimina o risco de que uma modificação da permissão do IAM ou uma alteração na política do bucket do S3 afete a operação do serviço.

Além de fornecer fontes de dados fundamentais, GuardDuty fornece recursos opcionais para identificar descobertas de segurança. Isso inclui proteção EKS, proteção RDS, proteção S3, proteção contra malware e proteção Lambda. Para novos detectores, esses recursos opcionais são ativados por padrão, exceto a Proteção EKS, que deve ser ativada manualmente.

- Com o GuardDuty S3 Protection, GuardDuty monitora os eventos de dados do Amazon S3, CloudTrail além dos eventos de gerenciamento CloudTrail padrão. O monitoramento de eventos de dados permite GuardDuty monitorar as operações de API em nível de objeto quanto a possíveis riscos de segurança dos dados em seus buckets do S3.
- GuardDuty A Proteção contra Malware detecta a presença de malware em instâncias do Amazon EC2 ou cargas de trabalho de contêineres iniciando escaneamentos sem agente em volumes anexados do Amazon Elastic Block Store (Amazon EBS). GuardDuty também detecta possíveis malwares em buckets do S3 examinando objetos recém-carregados ou novas versões de objetos existentes.
- GuardDuty O RDS Protection foi projetado para traçar o perfil e monitorar a atividade de acesso aos bancos de dados Amazon Aurora sem afetar o desempenho do banco de dados.
- GuardDuty O EKS Protection inclui o monitoramento do registro de auditoria e o monitoramento do tempo de execução do EKS. Com o EKS Audit Log Monitoring, GuardDuty monitora os

registros de auditoria do Kubernetes dos clusters do Amazon EKS e os analisa em busca de atividades potencialmente maliciosas e suspeitas. O EKS Runtime Monitoring usa o agente de GuardDuty segurança (que é um complemento do Amazon EKS) para fornecer visibilidade em tempo de execução de cargas de trabalho individuais do Amazon EKS. O agente GuardDuty de segurança ajuda a identificar contêineres específicos em seus clusters do Amazon EKS que estão potencialmente comprometidos. Ele também pode detectar tentativas de escalar privilégios de um contêiner individual para o host subjacente do Amazon EC2 ou para o ambiente mais amplo. AWS

GuardDuty também fornece um recurso conhecido como Detecção Estendida de Ameaças, que detecta automaticamente ataques em vários estágios que abrangem fontes de dados, vários tipos de AWS recursos e tempo dentro de um. Conta da AWS GuardDutycorrelaciona esses eventos, chamados de sinais, para identificar cenários que se apresentam como ameaças potenciais ao seu AWS ambiente e, em seguida, gera uma descoberta da sequência de ataque. Isso abrange cenários de ameaças que envolvem comprometimento relacionado ao uso indevido de AWS credenciais e tentativas de comprometimento de dados em seu. Contas da AWS GuardDuty considera todos os tipos de descoberta de sequências de ataque como críticos. Esse recurso é ativado por padrão e não há custo adicional associado a ele.

No AWS SRA, GuardDuty é ativado em todas as contas por meio de AWS Organizations, e todas as descobertas podem ser visualizadas e acionadas pelas equipes de segurança apropriadas na conta do administrador GuardDuty delegado (neste caso, a conta do Security Tooling). GuardDuty as descobertas ativas são exportadas para um bucket central do S3 na conta do Log Archive, para que você possa reter as descobertas por mais de 90 dias. As descobertas são exportadas da conta do administrador delegado e também incluem todas as descobertas das contas de membros associadas na mesma região. As descobertas no bucket do S3 são criptografadas com uma chave gerenciada pelo AWS KMS cliente. A política de bucket do S3 e a política de chaves do KMS são configuradas para permitir somente GuardDuty o uso dos recursos.

Quando AWS Security Hub CSPM ativado, GuardDuty as descobertas fluem automaticamente para o Security Hub CSPM e o Security Hub. Quando o Amazon Detective está ativado, GuardDuty as descobertas são incluídas no processo de ingestão de registros do Detective. GuardDuty e o Detective oferecem suporte a fluxos de trabalho de usuários de vários serviços, onde GuardDuty fornece links do console que redirecionam você de uma descoberta selecionada para uma página de Detetive que contém um conjunto selecionado de visualizações para investigar essa descoberta. Por exemplo, você também pode se integrar GuardDuty à Amazon EventBridge para automatizar as melhores práticas GuardDuty, como automatizar respostas a novas descobertas. GuardDuty

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação do GuardDuty. Inclui configuração criptografada do bucket S3, administração delegada e GuardDuty habilitação para todas as contas existentes e futuras na organização. AWS

AWS Config

AWS Configé um serviço que permite avaliar, auditar e avaliar as configurações dos AWS recursos suportados em seu Contas da AWS. AWS Config monitora e registra continuamente as configurações AWS dos recursos e avalia automaticamente as configurações gravadas em relação às configurações desejadas. Você também pode se integrar AWS Config a outros serviços para fazer o trabalho pesado em pipelines automatizados de auditoria e monitoramento. Por exemplo, AWS Config pode monitorar alterações em segredos individuais em AWS Secrets Manager.

Você pode avaliar as configurações de seus AWS recursos usando Regras do AWS Configo. AWS Config fornece uma biblioteca de regras personalizáveis e predefinidas chamadas regras gerenciadas, ou você pode criar suas próprias regras personalizadas. Você pode executar Regras do AWS Config no modo proativo (antes da implantação dos recursos) ou no modo detetive (após a implantação dos recursos). Os recursos podem ser avaliados quando há alterações na configuração, em um cronograma periódico ou em ambos.

Um pacote de conformidade é um conjunto de AWS Config regras e ações de remediação que podem ser implantadas como uma única entidade em uma conta e região, ou em uma organização em. AWS Organizations Os pacotes de conformidade são criados por meio da criação de um modelo YAML que contém a lista de regras AWS Config gerenciadas ou personalizadas e ações de correção. Para começar a avaliar seu AWS ambiente, use um dos exemplos de modelos de pacote de conformidade.

AWS Config se integra AWS Security Hub CSPM para enviar os resultados das avaliações de regras AWS Config gerenciadas e personalizadas como descobertas para o Security Hub CSPM.

Regras do AWS Config pode ser usado em conjunto com AWS Systems Manager a correção eficaz de recursos não compatíveis. Você usa o Systems Manager Explorer para coletar o status de conformidade das AWS Config regras em seu Contas da AWS cross Regiões da AWS e, em seguida, usa os documentos (runbooks) do Systems Manager Automation para resolver suas regras não compatíveis AWS Config . Para obter detalhes sobre a implementação, consulte a postagem

do blog Corrija AWS Config regras não compatíveis com AWS Systems Manager runbooks de automação.

O AWS Config agregador coleta dados de configuração e conformidade em várias contas, regiões e organizações em. AWS Organizations O painel do agregador exibe os dados de configuração dos recursos agregados. Os painéis de inventário e conformidade oferecem informações essenciais e atuais sobre suas configurações de AWS recursos e status de conformidade em toda Contas da AWS Regiões da AWS, dentro ou fora de uma AWS organização. Eles permitem que você visualize e avalie seu inventário de AWS recursos sem precisar escrever consultas AWS Config avançadas. Você pode obter informações essenciais, como um resumo da conformidade por recursos, as 10 principais contas que têm recursos não compatíveis, uma comparação de instâncias EC2 em execução e interrompidas por tipo e volumes do EBS por tipo e tamanho de volume.

Se você usa AWS Control Tower para gerenciar sua AWS organização, ele implantará um conjunto de AWS Config regras como proteções de detetive (categorizadas como obrigatórias, altamente recomendadas ou eletivas). Essas grades de proteção ajudam você a governar seus recursos e monitorar a conformidade em todas as contas da sua organização. AWS Essas AWS Config regras usarão automaticamente uma `aws-control-tower` tag que tenha um valor de`managed-by-control-tower`.

AWS Config deve estar habilitada para cada conta de membro na AWS organização e Região da AWS que contenha os recursos que você deseja proteger. Você pode gerenciar centralmente (por exemplo, criar, atualizar e excluir) AWS Config as regras em todas as contas da sua AWS organização. Na conta de administrador AWS Config delegado, você pode implantar um conjunto comum de AWS Config regras em todas as contas e especificar contas nas quais AWS Config as regras não devem ser criadas. A conta de administrador AWS Config delegado também pode agregar dados de configuração e conformidade de recursos de todas as contas dos membros para fornecer uma visão única. Use o APIs da conta de administrador delegado para impor a governança, garantindo que as AWS Config regras subjacentes não possam ser modificadas pelas contas dos membros em sua AWS organização. AWS Config é nativamente integrado para enviar descobertas AWS Security Hub CSPM, se o CSPM do Security Hub estiver ativado e existir pelo menos uma regra AWS Config gerenciada ou personalizada.

No AWS SRA, a conta do administrador AWS Config delegado é a conta do Security Tooling. O canal AWS Config de entrega é configurado para fornecer instantâneos de configuração de recursos em um bucket S3 centralizado na conta do Log Archive. Como a conta do Log Archive é o repositório central de registros, ela é usada para armazenar a configuração de recursos.

Considerações sobre design

- AWS Config transmite notificações de alteração de configuração e conformidade para a Amazon EventBridge. Isso significa que você pode usar os recursos de filtragem nativos EventBridge para filtrar AWS Config eventos e rotear tipos específicos de notificações para alvos específicos. Por exemplo, você pode enviar notificações de conformidade de regras específicas ou tipos de recursos para endereços de e-mail específicos ou rotear notificações de alteração de configuração para uma ferramenta externa de gerenciamento de serviços de TI (ITSM) ou banco de dados de gerenciamento de configuração (CMDB). Para obter mais informações, consulte as AWS Config melhores práticas da publicação no blog.
- Além de usar a avaliação AWS Config proativa de regras, você pode usar AWS CloudFormation Guard, que é uma ferramenta de policy-as-code avaliação que verifica proativamente a conformidade da configuração de recursos. A interface de linha de AWS CloudFormation Guard comando (CLI) fornece uma linguagem declarativa e específica de domínio (DSL) que você pode usar para expressar políticas como código. Além disso, você pode usar AWS CLI comandos para validar dados estruturados em formato JSON ou YAML, como conjuntos de CloudFormation alterações, arquivos de configuração do Terraform baseados em JSON ou configurações do Kubernetes. Você pode executar as avaliações localmente usando a AWS CloudFormation Guard CLI como parte do seu processo de criação ou executá-la em seu pipeline de implantação. Se você tiver AWS Cloud Development Kit (AWS CDK)aplicativos, poderá usar o cdk-nag para verificar proativamente as melhores práticas.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação que implanta pacotes de AWS Config conformidade em todas as Contas da AWS regiões de uma organização. AWS O módulo AWS Config Agregador ajuda você a configurar um AWS Config agregador delegando a administração a uma conta de membro (Ferramentas de Segurança) na conta de Gerenciamento da Organização e, em seguida, configurando o AWS Config Agregador na conta de administrador delegado para todas as contas existentes e futuras na organização. AWS Você pode usar o módulo AWS Config Control Tower

Management Account para ativar a conta de gerenciamento da AWS Config organização – ele não está ativado pelo. AWS Control Tower

Amazon Security Lake

O Amazon Security Lake é um serviço de data lake de segurança totalmente gerenciado. Você pode usar o Security Lake para centralizar automaticamente os dados de segurança de AWS ambientes, fornecedores de software como serviço (SaaS), locais e fontes terceirizadas. O Security Lake ajuda você a criar uma fonte de dados normalizada que simplifica o uso de ferramentas de análise em relação aos dados de segurança, para que você possa obter uma compreensão mais completa de sua postura de segurança em toda a organização. O data lake é respaldado pelos buckets do Amazon Simple Storage Service (Amazon S3). Você é o proprietário dos seus dados. O Security Lake coleta automaticamente registros de Serviços da AWS, incluindo AWS CloudTrail, Amazon VPC, Amazon Route 53, Amazon S3, registros de auditoria AWS Lambda, descobertas e AWS Security Hub CSPM registros do Amazon EKS. AWS WAF

AWS A SRA recomenda que você use a conta do Log Archive como a conta de administrador delegado do Security Lake. Para obter mais informações sobre como configurar a conta de administrador delegado, consulte Amazon Security Lake na seção Security OU – Log Archive account. As equipes de segurança que desejam acessar os dados do Security Lake ou precisam gravar registros não nativos nos buckets do Security Lake usando funções personalizadas de extração, transformação e carregamento (ETL) devem operar na conta do Security Tooling.

O Security Lake pode coletar registros de diferentes provedores de nuvem, registros de soluções de terceiros ou outros registros personalizados. Recomendamos que você use a conta do Security Tooling para executar as funções ETL para converter os registros para o formato Open Cybersecurity Schema Framework (OCSF) e gerar um arquivo no formato Apache Parquet. O Security Lake cria a função entre contas com as permissões adequadas para a conta do Security Tooling e a fonte personalizada apoiada por funções ou AWS Glue rastreadores Lambda, para gravar dados nos buckets S3 do Security Lake.

O administrador do Security Lake deve configurar as equipes de segurança que usam a conta do Security Tooling e exigir acesso aos registros que o Security Lake coleta como assinantes. O Security Lake oferece suporte a dois tipos de acesso de assinantes:

- Acesso aos dados — Os assinantes podem acessar diretamente os objetos do Amazon S3 para o Security Lake. O Security Lake gerencia a infraestrutura e as permissões. Quando você configura

a conta do Security Tooling como assinante de acesso a dados do Security Lake, a conta é notificada sobre novos objetos nos buckets do Security Lake por meio do Amazon Simple Queue Service (Amazon SQS), e o Security Lake cria as permissões para acessar esses novos objetos.

- Acesso à consulta — Os assinantes podem consultar dados de origem de AWS Lake Formation tabelas em seu bucket do S3 usando serviços como o Amazon Athena. O acesso entre contas é configurado automaticamente para acesso a consultas usando o Lake Formation. Quando você configura a conta do Security Tooling como assinante de acesso a consultas do Security Lake, a conta recebe acesso somente de leitura aos registros na conta do Security Lake. Quando você usa esse tipo de assinante, o Athena AWS Glue e as tabelas são compartilhadas da conta do Security Lake Log Archive com a conta do Security Tooling por meio de (). AWS Resource Access Manager AWS RAM Para habilitar esse recurso, você precisa atualizar as configurações de compartilhamento de dados entre contas para a versão 3.

Para obter mais informações sobre a criação de assinantes, consulte Gerenciamento de assinantes na documentação do Security Lake.

Para obter as melhores práticas para ingerir fontes personalizadas, consulte Coleta de dados de fontes personalizadas na documentação do Security Lake.

Você pode usar o Amazon Quick Sight, o Amazon OpenSearch Service e SageMaker o Amazon para configurar análises com base nos dados de segurança que você armazena no Security Lake.

> **Considerações sobre design**
>
> Se uma equipe de aplicativos precisar consultar os dados do Security Lake para atender a um requisito comercial, o administrador do Security Lake deverá configurar essa conta do aplicativo como assinante.

Amazon Macie

O Amazon Macie é um serviço totalmente gerenciado de segurança e privacidade de dados que usa aprendizado de máquina e correspondência de padrões para descobrir e ajudar a proteger seus dados confidenciais em. AWS Você precisa identificar o tipo e a classificação dos dados que sua carga de trabalho está processando para garantir que os controles apropriados sejam aplicados. Você pode usar o Macie para automatizar a descoberta e a emissão de relatórios de dados confidenciais de duas maneiras: realizando a descoberta automatizada de dados confidenciais

e criando e executando trabalhos de descoberta de dados confidenciais. Com a descoberta automatizada de dados confidenciais, o Macie avalia seu inventário de buckets do S3 diariamente e usa técnicas de amostragem para identificar e selecionar objetos representativos do S3 de seus buckets. Em seguida, o Macie recupera e analisa os objetos selecionados, inspecionando-os em busca de dados confidenciais. Trabalhos confidenciais de descoberta de dados fornecem análises mais detalhadas e direcionadas. Com essa opção, você define a amplitude e a profundidade da análise, incluindo os compartimentos do S3 a serem analisados, a profundidade da amostragem e os critérios personalizados que derivam das propriedades dos objetos do S3. Se o Macie detectar um possível problema com a segurança ou a privacidade de um bucket, ele criará uma descoberta de política para você. A descoberta automatizada de dados é ativada por padrão para todos os novos clientes da Macie, e os clientes existentes da Macie podem habilitá-la com um clique.

O Macie está habilitado em todas as contas por meio de AWS Organizations. Os diretores que têm as permissões apropriadas na conta do administrador delegado (nesse caso, a conta do Security Tooling) podem ativar ou suspender o Macie em qualquer conta, criar trabalhos confidenciais de descoberta de dados para buckets pertencentes às contas dos membros e visualizar todas as descobertas de políticas de todas as contas dos membros. As descobertas de dados confidenciais só podem ser visualizadas pela conta que criou o trabalho de descobertas confidenciais. Para obter mais informações, consulte Gerenciando várias contas do Macie como uma organização na documentação do Macie.

As descobertas do Macie fluem AWS Security Hub CSPM para revisão e análise. O Macie também se integra EventBridge à Amazon para facilitar respostas automatizadas a descobertas, como alertas, feeds para sistemas de gerenciamento de eventos e informações de segurança (SIEM) e remediação automatizada.

Considerações sobre design

- Se os objetos do S3 forem criptografados com uma chave AWS Key Management Service (AWS KMS) gerenciada por você, você poderá adicionar a função vinculada ao serviço Macie como usuário-chave dessa chave KMS para permitir que o Macie escaneie os dados.
- O Macie é otimizado para escanear objetos no Amazon S3. Como resultado, qualquer tipo de objeto compatível com Macie que possa ser colocado no Amazon S3 (permanente ou temporariamente) pode ser escaneado em busca de dados confidenciais. Isso significa que dados de outras fontes — por exemplo, exportações periódicas de instantâneos dos bancos de dados Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora,

tabelas exportadas do Amazon DynamoDB ou arquivos de texto extraídos de aplicativos nativos ou de terceiros — podem ser movidos para o Amazon S3 e avaliados pelo Macie.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação do Amazon Macie. Isso inclui delegar a administração a uma conta de membro e configurar o Macie dentro da conta de administrador delegado para todas as contas existentes e futuras na organização. AWS O Macie também está configurado para enviar as descobertas para um bucket central do S3 que é criptografado com uma chave gerenciada pelo cliente. AWS KMS

IAM Access Analyzer

À medida que você acelera sua jornada de Nuvem AWS adoção e continua inovando, é fundamental manter um controle rígido sobre o acesso refinado (permissões), conter a proliferação de acesso e garantir que as permissões sejam usadas de forma eficaz. O acesso excessivo e não utilizado apresenta desafios de segurança e torna mais difícil para as empresas aplicarem o princípio do menor privilégio. Esse princípio é um importante pilar da arquitetura de segurança que envolve o dimensionamento contínuo das permissões do IAM para equilibrar os requisitos de segurança com os requisitos operacionais e de desenvolvimento de aplicativos. Esse esforço envolve várias partes interessadas, incluindo equipes centrais de segurança e Cloud Center of Excellence (CCoE), bem como equipes de desenvolvimento descentralizadas.

AWS Identity and Access Management O Access Analyzer fornece ferramentas para definir com eficiência permissões refinadas, verificar as permissões pretendidas e refinar as permissões removendo o acesso não utilizado para ajudá-lo a atender aos padrões de segurança da sua empresa. Ele oferece visibilidade do acesso externo e interno aos AWS recursos e das descobertas de acesso não utilizadas por meio de painéis e. AWS Security Hub CSPM Além disso, ele oferece suporte à Amazon EventBridge para fluxos de trabalho personalizados de notificação e remediação baseados em eventos.

O recurso de descobertas do analisador de acesso externo do IAM Access Analyzer ajuda você a identificar os recursos em sua AWS organização e contas, como buckets do Amazon S3 ou funções do IAM, que são compartilhados com uma entidade externa. A AWS organização ou conta que você escolher é conhecida como zona de confiança. O analisador usa raciocínio automatizado

para analisar todos os recursos suportados dentro da zona de confiança e gera descobertas para diretores que podem acessar os recursos de fora da zona de confiança. Essas descobertas ajudam a identificar recursos que são compartilhados com uma entidade externa e ajudam a visualizar como sua política afeta o acesso público e entre contas ao seu recurso antes de implantar as permissões do recurso. Isso está disponível sem custo adicional.

Da mesma forma, o recurso de localização do analisador de acesso interno do IAM Access Analyzer ajuda você a identificar os recursos em sua AWS organização e as contas que são compartilhadas com os diretores internamente em sua organização ou conta. Essa análise apóia o princípio do menor privilégio, garantindo que seus recursos especificados possam ser acessados somente pelos diretores pretendidos em sua organização. Esse é um recurso pago e requer configuração explícita de recursos para inspecionar. Use esse recurso criteriosamente para monitorar recursos confidenciais específicos que, por design, precisam ser bloqueados até mesmo internamente.

As descobertas do IAM Access Analyzer também ajudam você a identificar o acesso não utilizado concedido em suas AWS organizações e contas, incluindo:

- Funções do IAM não usadas — funções que não têm atividade de acesso dentro da janela de uso especificada.
- Usuários, credenciais e chaves de acesso não utilizados do IAM — Credenciais que pertencem aos usuários do IAM e são usadas para acesso Serviços da AWS e recursos.
- Políticas e permissões do IAM não usadas — permissões em nível de serviço e de ação que não foram usadas por uma função em uma janela de uso especificada. O IAM Access Analyzer usa políticas baseadas em identidade que são anexadas às funções para determinar os serviços e ações que essas funções podem acessar. O analisador fornece uma análise das permissões não utilizadas para todas as permissões de nível de serviço.

Você pode usar as descobertas geradas pelo IAM Access Analyzer para obter visibilidade e corrigir qualquer acesso não intencional ou não utilizado com base nas políticas e padrões de segurança da sua organização. Após a correção, essas descobertas são marcadas como resolvidas na próxima vez em que o analisador for executado. Se a descoberta for intencional, você pode marcá-la como arquivada no IAM Access Analyzer e priorizar outras descobertas que apresentem um maior risco de segurança. Além disso, você pode configurar regras de arquivamento para arquivar automaticamente descobertas específicas. Por exemplo, é possível criar uma regra de arquivamento para arquivar automaticamente qualquer descoberta de um bucket do Amazon S3 específico ao qual você concede acesso regularmente.

Como criador, você pode usar o IAM Access Analyzer para realizar verificações automatizadas de políticas do IAM no início do processo de desenvolvimento e implantação (CI/CD) para aderir aos padrões de segurança corporativos. Você pode integrar as verificações e análises de políticas personalizadas do IAM Access Analyzer AWS CloudFormation para automatizar as análises de políticas como parte dos pipelines da sua equipe de CI/CD desenvolvimento. Isso inclui:

- Validação de políticas do IAM — O IAM Access Analyzer valida suas políticas em relação à gramática e AWS às melhores práticas de políticas do IAM. Você pode ver as descobertas das verificações de validação de políticas, incluindo avisos de segurança, erros, avisos gerais e sugestões para sua política. Atualmente, mais de 100 verificações de validação de políticas estão disponíveis e podem ser automatizadas usando o AWS Command Line Interface (AWS CLI) APIs e.
- Verificações de políticas personalizadas do IAM — As verificações de políticas personalizadas do IAM Access Analyzer validam suas políticas de acordo com os padrões de segurança especificados. As verificações de políticas personalizadas usam raciocínio automatizado para fornecer um nível mais alto de garantia sobre o cumprimento dos padrões de segurança corporativos. Os tipos de verificações de políticas personalizadas incluem:
  - Compare com uma política de referência: ao editar uma política, você pode compará-la com uma política de referência, como uma versão existente da política, para verificar se a atualização concede novo acesso. A CheckNoNewAccessAPI compara duas políticas (uma política atualizada e uma política de referência) para determinar se a política atualizada introduz um novo acesso à política de referência e retorna uma resposta positiva ou negativa.
  - Compare uma lista de ações do IAM: você pode usar a CheckAccessNotGrantedAPI para garantir que uma política não conceda acesso a uma lista de ações críticas definidas em seu padrão de segurança. Essa API usa uma política e uma lista de até 100 ações do IAM para verificar se a política permite pelo menos uma das ações e retorna uma resposta positiva ou reprovada.

As equipes de segurança e outros autores de políticas do IAM podem usar o IAM Access Analyzer para criar políticas que estejam em conformidade com a gramática e os padrões de segurança das políticas do IAM. A criação manual de políticas do tamanho certo pode ser propensa a erros e demorada. O recurso de geração de políticas do IAM Access Analyzer ajuda na criação de políticas do IAM com base na atividade de acesso do principal. O IAM Access Analyzer analisa AWS CloudTrail os registros dos serviços compatíveis e gera um modelo de política que contém as permissões que foram usadas pelo diretor no intervalo de datas especificado. Em seguida, você

pode usar esse modelo para criar uma política com permissões refinadas que conceda somente as permissões necessárias.

- Você deve ter uma CloudTrail trilha ativada para que sua conta gere uma política com base na atividade de acesso.
- O IAM Access Analyzer não identifica atividades em nível de ação para eventos de dados, como eventos de dados do Amazon S3, nas políticas geradas.
- A `iam:PassRole` ação não é monitorada CloudTrail e não está incluída nas políticas geradas.

O IAM Access Analyzer é implantado na conta do Security Tooling por meio da funcionalidade de administrador delegado em. AWS Organizations O administrador delegado tem permissões para criar e gerenciar analisadores com a AWS organização como zona de confiança.

> **Considerações sobre design**
>
> Para obter descobertas do escopo da conta (onde a conta serve como limite confiável), você cria um analisador do escopo da conta em cada conta membro. Isso pode ser feito como parte do pipeline da conta. As descobertas do escopo da conta fluem para o CSPM do Security Hub no nível da conta do membro. De lá, eles fluem para a conta de administrador delegado do CSPM do Security Hub (Security Tooling).

> **Exemplos de implementação**
>
> - A biblioteca de códigos AWS SRA fornece um exemplo de implementação do IAM Access Analyzer. Ele demonstra como configurar um analisador em nível de organização em uma conta de administrador delegado e um analisador em nível de conta em cada conta.
> - Para obter informações sobre como você pode integrar verificações de políticas personalizadas aos fluxos de trabalho do construtor, consulte a postagem do AWS blog Apresentando as verificações de políticas personalizadas do IAM Access Analyzer.

AWS Firewall Manager

AWS Firewall Managerajuda a proteger sua rede simplificando suas tarefas de administração e manutenção para AWS WAF grupos AWS Network Firewall de segurança da Amazon VPC Amazon

Route 53 Resolver e DNS Firewall em várias contas e recursos. AWS Shield Advanced Com o Firewall Manager, você configura suas regras de AWS WAF firewall, proteções Shield Advanced, grupos de segurança da Amazon VPC, firewalls do Network Firewall e associações de grupos de regras do DNS Firewall somente uma vez. O serviço aplica automaticamente as regras e as proteções em todas as contas e recursos, mesmo na adição de novos recursos.

O Firewall Manager é particularmente útil quando você deseja proteger toda a AWS organização em vez de um pequeno número de contas e recursos específicos, ou se você adiciona frequentemente novos recursos que deseja proteger. O Firewall Manager usa políticas de segurança para permitir que você defina um conjunto de configurações, incluindo regras, proteções e ações relevantes que devem ser implantadas e as contas e os recursos (indicados por tags) a serem incluídos ou excluídos. Você pode criar configurações granulares e flexíveis e, ao mesmo tempo, expandir o controle para um grande número de contas e. VPCs Essas políticas aplicam de forma automática e consistente as regras que você configura, mesmo quando novas contas e recursos são criados. O Firewall Manager é ativado em todas as contas e a configuração e o gerenciamento são realizados pelas equipes de segurança apropriadas na conta de administrador delegado do Firewall Manager (nesse caso, a conta do Security Tooling). AWS Organizations

Você deve habilitar AWS Config para cada um Região da AWS que contenha os recursos que você deseja proteger. Se você não quiser habilitá-la AWS Config para todos os recursos, deverá habilitá-la para recursos associados ao tipo de política do Firewall Manager que você usa. Quando você usa o Firewall Manager AWS Security Hub CSPM e o Firewall Manager, o Firewall Manager envia automaticamente suas descobertas para o Security Hub CSPM. O Firewall Manager cria descobertas para recursos que estão fora de conformidade e para ataques que ele detecta, e envia as descobertas para o Security Hub CSPM. Ao configurar uma política do Firewall Manager para AWS WAF, você pode ativar centralmente o registro em listas de controle de acesso à web (web ACLs) para todas as contas dentro do escopo e centralizar os registros em uma única conta.

Com o Firewall Manager, você pode ter um ou vários administradores que podem gerenciar os recursos de firewall da sua organização. Ao atribuir vários administradores, você pode aplicar condições restritivas de escopo administrativo para definir os recursos (contas, regiões OUs, tipos de política) que cada administrador pode gerenciar. Isso lhe dá a flexibilidade de ter diferentes funções de administrador em sua organização e ajuda a manter a entidade principal do acesso de privilégio mínimo. O AWS SRA usa um administrador com escopo administrativo completo delegado à conta do Security Tooling.

Considerações sobre design

Os gerentes de contas de membros individuais na AWS organização podem configurar controles adicionais (como AWS WAF regras e grupos de segurança da Amazon VPC) nos serviços gerenciados do Firewall Manager de acordo com suas necessidades específicas.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação do Firewall Manager. Ele demonstra a administração delegada (ferramentas de segurança), implanta um grupo de segurança máximo permitido, configura uma política de grupo de segurança e configura várias políticas. AWS WAF

Amazon EventBridge

EventBridgeA Amazon é um serviço de barramento de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes. É frequentemente usado na automação de segurança. Você pode configurar regras de roteamento para determinar para onde enviar seus dados para criar arquiteturas de aplicativos que reajam em tempo real a todas as suas fontes de dados. Você pode criar um barramento de eventos personalizado para receber eventos de seus aplicativos personalizados, além de usar o barramento de eventos padrão em cada conta. Você pode criar um barramento de eventos na conta do Security Tooling que pode receber eventos específicos de segurança de outras contas na organização. AWS Por exemplo, ao vincular Regras do AWS Config Amazon e AWS Security Hub CSPM com GuardDuty EventBridge, você cria um pipeline flexível e automatizado para rotear dados de segurança, gerar alertas e gerenciar ações para resolver problemas.

Considerações sobre design

- EventBridge é capaz de rotear eventos para vários alvos diferentes. Um padrão valioso para automatizar ações de segurança é conectar eventos específicos a AWS Lambda respondentes individuais, que tomam as medidas apropriadas. Por exemplo, em determinadas circunstâncias, talvez você queira usar para EventBridge rotear uma descoberta pública de bucket do S3 para um respondente Lambda que corrige a política

do bucket e remove as permissões públicas. Esses respondentes podem ser integrados aos seus manuais e manuais investigativos para coordenar as atividades de resposta.

- Uma prática recomendada para uma equipe de operações de segurança bem-sucedida é integrar o fluxo de eventos e descobertas de segurança em um sistema de notificação e fluxo de trabalho, como um sistema de emissão de bilhetes, um bug/issue sistema ou outro sistema de gerenciamento de informações e eventos de segurança (SIEM). Isso elimina o fluxo de trabalho de e-mails e relatórios estáticos e ajuda você a rotear, escalar e gerenciar eventos ou descobertas. As habilidades de roteamento flexível do EventBridge são um poderoso facilitador dessa integração.

Amazon Detective

O Amazon Detective apoia sua estratégia responsiva de controle de segurança, facilitando a análise, a investigação e a identificação rápida da causa raiz das descobertas de segurança ou atividades suspeitas para seus analistas de segurança. Detective extrai automaticamente eventos baseados em tempo, como tentativas de login, chamadas de API e tráfego de rede dos registros e registros de fluxo AWS CloudTrail da Amazon VPC. Detective consome esses eventos usando fluxos independentes de registros e registros de fluxo CloudTrail da Amazon VPC. Você pode usar o Detective para acessar até um ano de dados históricos de eventos. Detective usa aprendizado de máquina e visualização para criar uma visão unificada e interativa do comportamento de seus recursos e das interações entre eles ao longo do tempo. Isso é chamado de gráfico de comportamento. Você pode explorar o gráfico de comportamento para examinar ações diferentes, como tentativas de login malsucedidas ou chamadas de API suspeitas.

O Detective se integra ao Amazon Security Lake para permitir que analistas de segurança consultem e recuperem registros armazenados no Security Lake. Você pode usar essa integração para obter informações adicionais dos CloudTrail registros e dos registros de fluxo da Amazon VPC que são armazenados no Security Lake enquanto conduz investigações de segurança no Detective.

Detective também ingere descobertas detectadas pela Amazon GuardDuty, incluindo ameaças detectadas pelo GuardDuty Runtime Monitoring. Quando uma conta ativa o Detective, ela se torna a conta de administrador do gráfico de comportamento. Antes de tentar ativar o Detective, certifique-se de que sua conta esteja cadastrada há GuardDuty pelo menos 48 horas. Se você não atender a esse requisito, não poderá habilitar DetectiveDetective.

Outras fontes de dados opcionais para Detective incluem registros de auditoria do Amazon EKS e. AWS Security Hub CSPM A fonte de dados do log de auditoria do Amazon EKS aprimora as informações fornecidas sobre os seguintes tipos de entidade: clusters do Amazon EKS, pods do Kubernetes, imagens de contêineres e assuntos do Kubernetes. A fonte de dados do Security Hub faz parte das descobertas de AWS segurança, onde correlaciona as descobertas de todos os produtos no Security Hub e as ingere no Detective.

Detective agrupa automaticamente várias descobertas relacionadas a um único evento de comprometimento de segurança em grupos de busca. Os agentes de ameaças geralmente realizam uma sequência de ações que levam a várias descobertas de segurança distribuídas ao longo do tempo e dos recursos. Portanto, encontrar grupos deve ser o ponto de partida para investigações que envolvam várias entidades e descobertas. Detective também fornece resumos de busca de grupos usando IA generativa que analisa automaticamente a localização de grupos e fornece informações em linguagem natural para ajudá-lo a acelerar as investigações de segurança.

Detective se integra com. AWS Organizations A conta de Gerenciamento da Organização delega uma conta de membro como a conta de administrador do Detective. No AWS SRA, essa é a conta do Security Tooling. A conta de administrador de Detective tem a capacidade de habilitar automaticamente todas as contas de membros atuais da organização como contas de membros de Detective e também adicionar novas contas de membros à medida que elas são adicionadas à organização. AWS As contas de administrador Detective também podem convidar contas de membros que atualmente não residem na AWS organização, mas estão na mesma região, a contribuir com seus dados para o gráfico de comportamento da conta principal. Quando uma conta de membro aceita o convite e é ativada, o Detective começa a ingerir e extrair os dados da conta do membro nesse gráfico de comportamento.

> **Considerações sobre design**
>
> Você pode navegar até Detective encontrando perfis nos consoles GuardDuty e. AWS Security Hub CSPM Esses links podem ajudar a agilizar o processo de investigação. Sua conta deve ser a conta administrativa do Detective e do serviço do qual você está migrando (ou do Security GuardDuty Hub CSPM). Se as contas principais forem as mesmas para os serviços, os links de integração funcionarão perfeitamente.

AWS Audit Manager

AWS Audit Managerajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia as auditorias e a conformidade com os regulamentos e padrões do setor. Ele permite que você passe da coleta, revisão e gerenciamento manual de evidências para uma solução que automatiza a coleta de evidências, fornece uma maneira simples de rastrear a origem das evidências de auditoria, permite a colaboração do trabalho em equipe e ajuda a gerenciar a segurança e a integridade das evidências. Quando é hora de uma auditoria, o Audit Manager ajuda você a gerenciar as análises de seus controles pelas partes interessadas.

Com o Audit Manager, você pode auditar com base em estruturas pré-criadas, como o benchmark Center for Internet Security (CIS), o CIS AWS Foundations Benchmark, System and Organization Controls 2 (SOC 2) e o Payment Card Industry Data Security Standard (PCI DSS). Também oferece a capacidade de criar suas próprias estruturas com controles padrão ou personalizados com base em seus requisitos específicos para auditorias internas.

O Audit Manager coleta quatro tipos de evidências. Três tipos de evidência são automatizados: evidência de verificação de conformidade de AWS Config e AWS Security Hub CSPM, evidência de eventos de gerenciamento de AWS CloudTrail e evidência de configuração de chamadas de AWS service-to-service API. Para evidências que não podem ser automatizadas, o Audit Manager permite que você faça upload de evidências manuais.

Por padrão, seus dados no Audit Manager são criptografados usando chaves AWS gerenciadas. O AWS SRA usa uma chave gerenciada pelo cliente para criptografia a fim de fornecer maior controle sobre o acesso lógico. Você também deve configurar um bucket do S3 no local em Região da AWS que o Audit Manager publica o relatório de avaliação. Esses buckets devem ser criptografados com uma chave gerenciada pelo cliente e ter uma política de bucket configurada para permitir que somente o Audit Manager publique relatórios.

> **Note**
>
> O Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com padrões e regulamentos de conformidade específicos. No entanto, ele não avalia sua conformidade. Portanto, as evidências coletadas pelo Audit Manager podem não incluir detalhes de seus processos operacionais necessários para auditorias. O Audit Manager não substitui o advogado ou os especialistas em conformidade. Recomendamos que

você contrate os serviços de um avaliador terceirizado certificado pelas estruturas de conformidade com as quais você é avaliado.

As avaliações do Audit Manager podem ser executadas em várias contas em suas AWS organizações. O Audit Manager coleta e consolida evidências em uma conta de administrador delegado em. AWS Organizations Essa funcionalidade de auditoria é usada principalmente pelas equipes de conformidade e auditoria interna e requer apenas acesso de leitura ao seu Contas da AWS.

Considerações sobre design

- O Audit Manager complementa outros serviços AWS de segurança AWS Security Hub CSPM, como AWS Security Hub, e AWS Config para ajudar a implementar uma estrutura de gerenciamento de riscos. O Audit Manager fornece funcionalidade independente de garantia de risco, enquanto o Security Hub CSPM ajuda você a supervisionar seus riscos e os pacotes de AWS Config conformidade auxiliam no gerenciamento de seus riscos. Profissionais de auditoria que estão familiarizados com o Modelo de Três Linhas desenvolvido pelo Instituto de Auditores Internos (IIA) devem observar que essa combinação Serviços da AWS ajuda você a cobrir as três linhas de defesa. Para obter mais informações, consulte a série de blogs em duas partes no blog Nuvem AWS Operations & Migrations.
- Para que o Audit Manager colete evidências de CSPM do Security Hub, a conta de administrador delegado para ambos os serviços precisa ser a mesma. Conta da AWS Por esse motivo, no AWS SRA, a conta do Security Tooling é o administrador delegado do Audit Manager.

AWS Artifact

AWS Artifacté hospedado na conta do Security Tooling para separar a funcionalidade de gerenciamento de artefatos de conformidade da conta de gerenciamento da AWS organização. Essa separação de tarefas é importante porque recomendamos que você evite usar a conta de gerenciamento da AWS organização para implantações, a menos que seja absolutamente necessário. Em vez disso, transmita as implantações para as contas dos membros. Como o gerenciamento de artefatos de auditoria pode ser feito a partir de uma conta de membro e a função

está estreitamente alinhada com a equipe de segurança e conformidade, a conta do Security Tooling é designada como a conta do administrador para. AWS Artifact Você pode usar AWS Artifact relatórios para baixar documentos de AWS segurança e conformidade, como certificações AWS ISO, PCI (Payment Card Industry) e relatórios de System and Organization Controls (SOC).

AWS Artifact não oferece suporte ao recurso de administração delegada. Em vez disso, você pode restringir esse recurso apenas às funções do IAM na conta do Security Tooling que pertencem às suas equipes de auditoria e conformidade, para que elas possam baixar, revisar e fornecer esses relatórios aos auditores externos conforme necessário. Além disso, você pode restringir funções específicas do IAM para ter acesso somente a AWS Artifact relatórios específicos por meio de políticas do IAM. Para exemplos de políticas do IAM, consulte a AWS Artifact documentação.

> **Considerações sobre design**
>
> Se você optar Conta da AWS por ter uma dedicada às equipes de auditoria e conformidade, poderá hospedar AWS Artifact em uma conta de auditoria de segurança, que é separada da conta do Security Tooling. AWS Artifact os relatórios fornecem evidências que demonstram que uma organização está seguindo um processo documentado ou atendendo a um requisito específico. Os artefatos de auditoria são coletados e arquivados em todo o ciclo de vida do desenvolvimento do sistema e podem ser usados como evidência em auditorias e avaliações internas ou externas.

AWS KMS

AWS Key Management Service(AWS KMS) ajuda você a criar e gerenciar chaves criptográficas e controlar seu uso em uma ampla variedade de Serviços da AWS e em seus aplicativos. AWS KMS é um serviço seguro e resiliente que usa módulos de segurança de hardware para proteger chaves criptográficas. Ele segue os processos de ciclo de vida padrão do setor para materiais essenciais, como armazenamento, rotação e controle de acesso às chaves. AWS KMS podem ajudar a proteger seus dados com chaves de criptografia e assinatura e podem ser usadas tanto para criptografia do lado do servidor quanto para criptografia do lado do cliente por meio do SDK de criptografia.AWS Para proteção e flexibilidade, AWS KMS oferece suporte a três tipos de chaves: chaves gerenciadas pelo cliente, chaves AWS gerenciadas e chaves AWS próprias. As chaves gerenciadas pelo cliente são AWS KMS chaves Conta da AWS que você cria, possui e gerencia. AWS chaves gerenciadas são AWS KMS chaves em sua conta que são criadas, gerenciadas e usadas em seu nome por uma AWS service (Serviço da AWS) que está integrada AWS KMS a. AWS chaves de propriedade

são uma coleção de AWS KMS chaves que uma pessoa AWS service (Serviço da AWS) possui e gerencia para uso em várias Contas da AWS. Para obter mais informações sobre o uso de AWS KMS chaves, consulte a AWS KMS documentação e os detalhes AWS KMS criptográficos.

Uma opção de implantação é centralizar a responsabilidade do gerenciamento de AWS KMS chaves em uma única conta e, ao mesmo tempo, delegar a capacidade de usar chaves na conta do aplicativo pelos recursos do aplicativo usando uma combinação de políticas de chave e IAM. Essa abordagem é segura e fácil de gerenciar, mas você pode encontrar obstáculos devido aos limites de AWS KMS limitação, aos limites do serviço da conta e à inundação da equipe de segurança com tarefas operacionais de gerenciamento de chaves. Outra opção de implantação é ter um modelo descentralizado no qual você permita AWS KMS residir em várias contas e permitir que os responsáveis pela infraestrutura e pelas cargas de trabalho em uma conta específica gerenciem suas próprias chaves. Esse modelo oferece às suas equipes de carga de trabalho mais controle, flexibilidade e agilidade sobre o uso de chaves de criptografia. Também ajuda a evitar limites de API, limita o escopo do impacto a Conta da AWS apenas um e simplifica relatórios, auditorias e outras tarefas relacionadas à conformidade. Em um modelo descentralizado, é importante implantar e aplicar grades de proteção para que as chaves descentralizadas sejam gerenciadas da mesma forma e o uso das AWS KMS chaves seja auditado de acordo com as melhores práticas e políticas estabelecidas. Para obter mais informações, consulte o whitepaper AWS Key Management Service Best Practices. AWS A SRA recomenda um modelo distribuído de gerenciamento de chaves no qual as AWS KMS chaves residam localmente na conta em que são usadas. Recomendamos que você evite usar uma única chave em uma conta para todas as funções criptográficas. As chaves podem ser criadas com base nos requisitos de função e proteção de dados e para aplicar o princípio do menor privilégio. Em alguns casos, as permissões de criptografia seriam mantidas separadas das permissões de descriptografia, e os administradores gerenciariam as funções do ciclo de vida, mas não conseguiriam criptografar ou descriptografar dados com as chaves que gerenciam.

Na conta do Security Tooling, AWS KMS é usado para gerenciar a criptografia de serviços de segurança centralizados, como a trilha da AWS CloudTrail organização que é gerenciada pela AWS organização.

CA Privada da AWS

Autoridade de Certificação Privada da AWS(CA Privada da AWS) é um serviço gerenciado de CA privada que ajuda você a gerenciar com segurança o ciclo de vida de seus certificados TLS de entidade final privada para instâncias EC2, contêineres, dispositivos de IoT e recursos locais. Ele permite comunicações TLS criptografadas para aplicativos em execução. Com CA Privada da AWS, você pode criar sua própria hierarquia de CA (uma CA raiz, por meio de subordinada

CAs, até certificados de entidade final) e emitir certificados com ela para autenticar usuários internos, computadores, aplicativos, serviços, servidores e outros dispositivos e assinar códigos de computador. Os certificados emitidos por uma CA privada são confiáveis somente na sua AWS organização, não na Internet.

Uma infraestrutura de chave pública (PKI) ou equipe de segurança pode ser responsável pelo gerenciamento de toda a infraestrutura de PKI. Isso inclui o gerenciamento e a criação da CA privada. No entanto, deve haver uma provisão que permita que as equipes de carga de trabalho atendam por conta própria aos requisitos de certificado. O AWS SRA descreve uma hierarquia centralizada de CA na qual a CA raiz está hospedada na conta do Security Tooling. Isso permite que as equipes de segurança apliquem um controle de segurança rigoroso, porque a CA raiz é a base de toda a PKI. No entanto, a criação de certificados privados da CA privada é delegada às equipes de desenvolvimento de aplicativos compartilhando a CA em uma conta de aplicativo usando AWS Resource Access Manager (AWS RAM). AWS RAM gerencia as permissões necessárias para o compartilhamento entre contas. Isso elimina a necessidade de uma CA privada em cada conta e fornece uma forma mais econômica de implantação. Para obter mais informações sobre o fluxo de trabalho e a implementação, consulte a postagem do blog Como usar AWS RAM para compartilhar sua CA Privada da AWS conta cruzada.

Note

AWS Certificate Manager (ACM) também ajuda você a provisionar, gerenciar e implantar certificados TLS públicos para uso com. Serviços da AWS Para oferecer suporte a essa funcionalidade, o ACM precisa residir no Conta da AWS que usaria o certificado público. Isso será discutido posteriormente neste guia, na seção Conta do aplicativo.

Considerações sobre design

- Com CA Privada da AWS, você pode criar uma hierarquia de autoridades de certificação com até cinco níveis. Você também pode criar várias hierarquias, cada uma com sua própria raiz. A CA Privada da AWS hierarquia deve seguir o design de PKI da sua organização. No entanto, lembre-se de que o aumento da hierarquia da CA aumenta o número de certificados no caminho de certificação, o que, por sua vez, aumenta o tempo de validação de um certificado de entidade final. Uma hierarquia de CA bem definida fornece benefícios que incluem controle de segurança granular apropriado para cada CA, delegação de CA subordinada a um aplicativo diferente, o que leva à divisão de tarefas

administrativas, uso de CA com confiança revogável limitada, a capacidade de definir diferentes períodos de validade e a capacidade de impor limites de caminho. Idealmente, sua raiz e seu subordinado CAs estão separados Contas da AWS. Para obter mais informações sobre como planejar uma hierarquia de CA usando CA Privada da AWS, consulte a CA Privada da AWS documentação e a postagem do blog Como proteger uma CA Privada da AWS hierarquia de escala corporativa para o setor automotivo e de manufatura.

- CA Privada da AWS pode se integrar à sua hierarquia de CA existente, o que permite que você use a capacidade de automação e AWS integração nativa do ACM em conjunto com a raiz de confiança existente que você usa atualmente. Você pode criar uma CA subordinada CA Privada da AWS apoiada por uma CA principal no local. Para obter mais informações sobre a implementação, consulte Instalando um certificado de CA subordinado assinado por uma CA externa principal na CA Privada da AWS documentação.

Amazon Inspector

O Amazon Inspector é um serviço automatizado de gerenciamento de vulnerabilidades que descobre e escaneia automaticamente instâncias do Amazon EC2, imagens de contêineres no Amazon Elastic Container Registry (Amazon AWS Lambda ECR), funções e repositórios de código em seus gerenciadores de código-fonte em busca de vulnerabilidades conhecidas de software e exposição não intencional na rede.

O Amazon Inspector avalia continuamente seu ambiente durante todo o ciclo de vida de seus recursos, examinando automaticamente os recursos sempre que você fizer alterações neles. Os eventos que iniciam a nova análise de um recurso incluem a instalação de um novo pacote em uma instância do EC2, a instalação de um patch e a publicação de um novo relatório de vulnerabilidades e exposições comuns (CVE) que afeta o recurso. O Amazon Inspector oferece suporte às avaliações de benchmark do Center of Internet Security (CIS) para sistemas operacionais em instâncias EC2.

O Amazon Inspector se integra com ferramentas de desenvolvedor, como Jenkins, e TeamCity para avaliações de imagens de contêineres. Você pode avaliar suas imagens de contêiner em busca de vulnerabilidades de software em sua integração contínua e entrega contínua (painel da CI/CD) tools, and push security to an earlier point in the software development lifecycle. Assessment findings are available in the CI/CD ferramenta), para que você possa realizar ações automatizadas em resposta a problemas críticos de segurança, como compilações bloqueadas ou envios de imagens para

registros de contêineres. Se você tiver um ativo Conta da AWS, você pode instalar o plug-in Amazon Inspector a partir do seu mercado de CI/CD ferramentas e adicionar um escaneamento do Amazon Inspector em seu pipeline de construção sem precisar ativar o serviço Amazon Inspector. Esse recurso funciona com CI/CD ferramentas hospedadas em qualquer lugar AWS, localmente ou em nuvens híbridas, para que você possa usar consistentemente uma única solução em todos os seus pipelines de desenvolvimento. Quando o Amazon Inspector é ativado, ele descobre automaticamente todas as suas instâncias do EC2, imagens de contêineres no Amazon ECR e nas ferramentas CI/CD e funções do Lambda em grande escala e as monitora continuamente em busca de vulnerabilidades conhecidas.

As descobertas de acessibilidade de rede do Amazon Inspector avaliam a acessibilidade de suas instâncias EC2 de ou para bordas de VPC, como gateways de internet, conexões de emparelhamento de VPC ou redes privadas virtuais () por meio de um gateway virtual. VPNs Essas regras ajudam a automatizar o monitoramento de suas AWS redes e a identificar onde o acesso à rede às suas instâncias do EC2 pode estar mal configurado por meio de grupos de segurança mal gerenciados, listas de controle de acesso (ACLs), gateways de internet e assim por diante. Para obter mais informações, consulte a documentação do Amazon Inspector.

Quando o Amazon Inspector identifica vulnerabilidades ou caminhos de rede abertos, ele produz uma descoberta que você pode investigar. A descoberta inclui detalhes abrangentes sobre a vulnerabilidade, incluindo uma pontuação de risco, o recurso afetado e recomendações de remediação. A pontuação de risco é adaptada especificamente ao seu ambiente e é calculada correlacionando as informações do up-to-date CVE com fatores temporais e ambientais, como informações de acessibilidade e explorabilidade da rede, para fornecer uma descoberta contextual.

O Amazon Inspector Code Security verifica o código-fonte do aplicativo primário, as dependências de aplicativos de terceiros e a infraestrutura como código (IaC) em busca de vulnerabilidades. Depois de ativar o Code Security, você pode criar e aplicar uma configuração de escaneamento ao seu repositório de código para determinar a frequência, o tipo de escaneamento e os repositórios a serem escaneados. O Code Security suporta testes estáticos de segurança de aplicativos (SAST), análise de composição de software (SCA) e escaneamento IaC. Para configurar a frequência, você pode definir escaneamentos sob demanda, em alterações de código ou periodicamente. A verificação de código captura trechos de código para destacar as vulnerabilidades detectadas. Os trechos de código são armazenados criptografados com chaves KMS. O administrador delegado de uma organização não pode visualizar trechos de código pertencentes a contas de membros. Depois de integrar seus gerenciadores de código-fonte (SCMs) com o Code Security, todos os repositórios de código são listados como projetos no console do Amazon Inspector. O Code

Security monitora somente a ramificação padrão de cada repositório. O Amazon Inspector simplifica a remediação de segurança fornecendo recomendações específicas de correção de código diretamente onde os desenvolvedores trabalham. A integração bidirecional com seu SCM sugere automaticamente correções como comentários nas solicitações pull (PRs) e nas solicitações de mesclagem (MRs) para descobertas críticas e importantes, além de alertar os desenvolvedores sobre as vulnerabilidades mais importantes a serem abordadas sem interromper o fluxo de trabalho.

Para verificar vulnerabilidades, as instâncias do EC2 devem ser gerenciadas AWS Systems Manager usando o AWS Systems Manager Agent (SSMAgent). Nenhum agente é necessário para a acessibilidade de rede de instâncias do EC2 ou para a verificação de vulnerabilidades de imagens de contêineres nas funções Amazon ECR ou Lambda.

O Amazon Inspector é integrado AWS Organizations e oferece suporte à administração delegada. No AWS SRA, a conta do Security Tooling é transformada em conta de administrador delegado para o Amazon Inspector. A conta de administrador delegado do Amazon Inspector pode gerenciar descobertas, dados e determinadas configurações para membros da organização. AWS Isso inclui visualizar os detalhes das descobertas agregadas de todas as contas dos membros, ativar ou desativar as verificações das contas dos membros e revisar os recursos escaneados dentro da organização. AWS

Considerações sobre design

- O Amazon Inspector se integra automaticamente com o Security AWS Security Hub CSPM Hub quando ambos os serviços estão habilitados. Você pode usar essa integração para enviar todas as descobertas do Amazon Inspector para o Security Hub CSPM, que então incluirá essas descobertas em sua análise da sua postura de segurança.
- O Amazon Inspector exporta automaticamente eventos para descobertas, alterações na cobertura de recursos e escaneamentos iniciais de recursos individuais para a Amazon e EventBridge, opcionalmente, para um bucket do Amazon Simple Storage Service (Amazon S3). Para exportar descobertas ativas para um bucket do S3, você precisa de uma AWS KMS chave que o Amazon Inspector possa usar para criptografar descobertas e de um bucket do S3 com permissões que permitam ao Amazon Inspector carregar objetos. EventBridgea integração permite monitorar e processar descobertas quase em tempo real como parte de seus fluxos de trabalho existentes de segurança e conformidade. EventBridge os eventos são publicados na conta de administrador delegado do Amazon Inspector, além da conta membro da qual eles se originaram.

- As integrações do Amazon Inspector Code Security com GitHub SaaS, GitHub Enterprise Cloud e GitHub Enterprise Server exigem acesso público à Internet.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação do Amazon Inspector. Ele demonstra a administração delegada (ferramentas de segurança) e configura o Amazon Inspector para todas as contas existentes e futuras na organização. AWS

AWS Security Incident Response

AWS Security Incident Responseé um serviço que ajuda você a se preparar e responder a incidentes de segurança em seu AWS ambiente. Ele faz a triagem das descobertas, escalona os eventos de segurança e gerencia casos que exigem sua atenção imediata. Além disso, dá acesso à Equipe de Resposta a Incidentes AWS do Cliente (CIRT), que investiga os recursos afetados. AWS Security Incident Response também fornece recursos automatizados de resposta e remediação por meio de AWS Systems Manager documentos (documentos SSM), que ajudam as equipes de segurança a responder e se recuperar de incidentes de segurança com mais eficiência. AWS Security Incident Response integra-se à Amazon GuardDuty e AWS Security Hub CSPM para receber descobertas de segurança e orquestrar respostas automatizadas.

No AWS SRA, AWS Security Incident Response é implantado na conta do Security Tooling como uma conta de administrador delegado. A conta do Security Tooling é selecionada porque está alinhada à finalidade da conta de operar serviços de segurança e automatizar alertas e respostas de segurança. A conta do Security Tooling também atua como a conta de administrador delegado do Security Hub CSPM e GuardDuty, além disso AWS Security Incident Response, ajuda a simplificar o gerenciamento do fluxo de trabalho. AWS Security Incident Response está configurado para funcionar com AWS Organizations, para que você possa gerenciar as respostas a incidentes nas contas da sua organização a partir da conta do Security Tooling.

AWS Security Incident Response ajuda você a implementar as seguintes fases do ciclo de vida de resposta a incidentes:

- Preparação: Crie e mantenha planos de resposta e documentos SSM para ações de contenção.

- Detecção e análise: analise automaticamente as descobertas de segurança e determine a gravidade do incidente.
- Detecção e análise: abra um caso suportado pelo serviço e entre em contato com o AWS CIRT para obter assistência adicional. O CIRT é um grupo de indivíduos que fornecem suporte durante eventos de segurança ativos.
- Contenção e erradicação: execute ações de contenção automatizadas por meio de documentos SSM.
- Atividade pós-incidente: documente os detalhes do incidente e conduza análises pós-incidentes.

Você também pode usar AWS Security Incident Response para criar casos autogerenciados. AWS Security Incident Response pode criar uma notificação ou um caso externo quando você precisa estar ciente ou agir sobre algo que possa afetar sua conta ou seus recursos. Esse recurso está disponível somente quando você ativa os fluxos de trabalho de resposta proativa e triagem de alertas como parte de sua assinatura.

Considerações sobre design

- Ao implementar AWS Security Incident Response, analise e teste cuidadosamente as ações de resposta automatizada antes de ativá-las na produção. A automação pode acelerar a resposta a incidentes, mas ações automatizadas configuradas incorretamente podem afetar cargas de trabalho legítimas.
- Considere usar documentos SSM AWS Security Incident Response para implementar procedimentos de contenção específicos da organização, mantendo as melhores práticas integradas do serviço para tipos comuns de incidentes.
- Se você planeja usar AWS Security Incident Response em uma VPC, certifique-se de ter os endpoints de VPC apropriados configurados para Systems Manager e outros serviços integrados para permitir ações de contenção em sub-redes privadas.

Implantando serviços de segurança comuns em todos Contas da AWS

A seção Aplicar serviços de segurança em sua AWS organização, anterior nesta referência Conta da AWS, destacou os serviços de segurança que protegem um e observou que muitos desses serviços também podem ser configurados e gerenciados em AWS Organizations. Alguns desses serviços devem ser implantados em todas as contas e você os verá no AWS SRA. Isso permite um conjunto

consistente de barreiras e fornece monitoramento, gerenciamento e governança centralizados em toda a organização. AWS

O Security Hub CSPM,, GuardDuty AWS Config, IAM Access Analyzer e as trilhas CloudTrail da organização aparecem em todas as contas. Os três primeiros oferecem suporte ao recurso de administrador delegado discutido anteriormente na seção A conta de gerenciamento, acesso confiável e administradores delegados. CloudTrail atualmente usa um mecanismo de agregação diferente.

O repositório de GitHub códigos AWS SRA fornece um exemplo de implementação para habilitar trilhas de CSPM,,, GuardDuty AWS Config AWS Firewall Manager, e CloudTrail organização do Security Hub em todas as suas contas, incluindo a conta de gerenciamento da AWS organização.

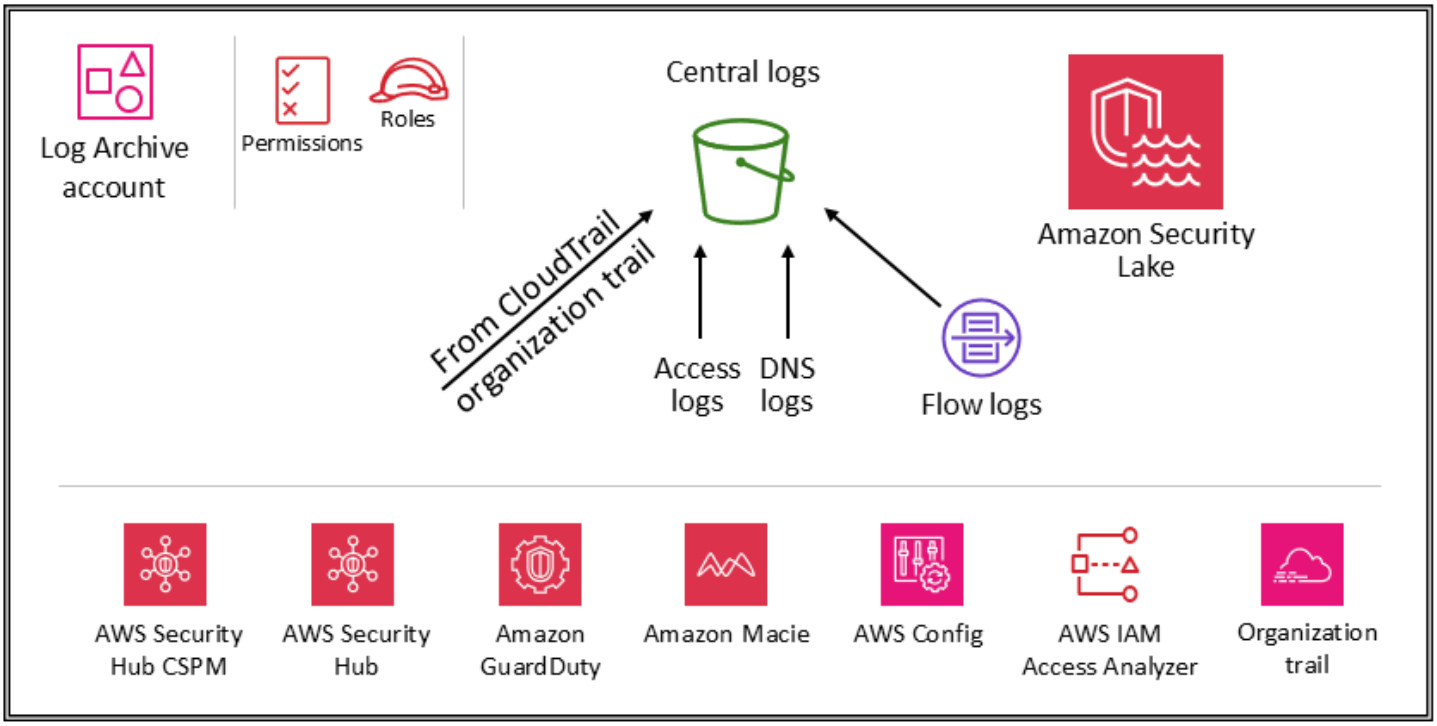
Considerações sobre design

- Configurações específicas da conta podem exigir serviços de segurança adicionais. Por exemplo, contas que gerenciam buckets do S3 (as contas Application e Log Archive) também devem incluir o Amazon Macie e considerar a ativação CloudTrail do registro de eventos de dados do S3 nesses serviços de segurança comuns. (O Macie oferece suporte à administração delegada com configuração e monitoramento centralizados.) Outro exemplo é o Amazon Inspector, que é aplicável somente para contas que hospedam instâncias EC2 ou imagens do Amazon ECR.
- Além dos serviços descritos anteriormente nesta seção, o AWS SRA inclui dois serviços focados em segurança, Amazon Detective e, que AWS Organizations oferecem suporte à integração AWS Audit Manager e à funcionalidade de administrador delegado. No entanto, eles não estão incluídos como parte dos serviços recomendados para a definição de base da conta, porque vimos que esses serviços são melhor usados nos seguintes cenários:
  - Você tem uma equipe dedicada ou um grupo de recursos que executam essas funções. O Detective é melhor utilizado pelas equipes de analistas de segurança e o Audit Manager é útil para suas equipes internas de auditoria ou conformidade.
  - Você quer se concentrar em um conjunto básico de ferramentas, como GuardDuty o Security Hub CSPM, no início do seu projeto e, em seguida, desenvolvê-las usando serviços que fornecem recursos adicionais.

UO de segurança | Conta do Log Archive

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços AWS de segurança que estão configurados na conta do Log Archive.



A conta Log Archive é dedicada à ingestão e arquivamento de todos os registros e backups relacionados à segurança. Com registros centralizados, você pode monitorar, auditar e alertar sobre o acesso a objetos do Amazon S3, atividades não autorizadas por identidades, mudanças na política do IAM e outras atividades críticas realizadas em recursos confidenciais. Os objetivos de segurança são simples: esse armazenamento deve ser imutável, acessado somente por mecanismos controlados, automatizados e monitorados, e criado para oferecer durabilidade (por exemplo, usando os processos apropriados de replicação e arquivamento). Os controles podem ser implementados em profundidade para proteger a integridade e a disponibilidade dos registros e do processo de gerenciamento de registros. Além dos controles preventivos, como atribuir funções de menor privilégio a serem usadas para acessar e criptografar registros com uma AWS KMS chave

controlada, use controles de detetive AWS Config para monitorar (alertar e corrigir) esse conjunto de permissões em caso de alterações inesperadas.

> **Considerações sobre design**
>
> Os dados de registro operacional usados por suas equipes de infraestrutura, operações e carga de trabalho geralmente se sobrepõem aos dados de registro usados pelas equipes de segurança, auditoria e conformidade. Recomendamos que você consolide seus dados operacionais de registro na conta do Log Archive. Com base em seus requisitos específicos de segurança e governança, talvez seja necessário filtrar os dados de registro operacionais salvos nessa conta. Talvez você também precise especificar quem tem acesso aos dados de registro operacionais na conta do Log Archive.

Tipos de registros

Os registros principais mostrados no AWS SRA incluem AWS CloudTrail (trilha da organização), registros de fluxo do Amazon VPC, registros de acesso da CloudFront Amazon AWS WAF e registros de DNS do Amazon Route 53. Esses registros fornecem uma auditoria das ações tomadas (ou tentadas) por um usuário AWS service (Serviço da AWS), função ou entidade de rede (identificadas, por exemplo, por um endereço IP). Outros tipos de registro (por exemplo, registros de aplicativos ou registros de banco de dados) também podem ser capturados e arquivados. Para obter mais informações sobre fontes de log e melhores práticas de registro, consulte a documentação de segurança de cada serviço.

Amazon S3 como armazenamento central de registros

Muitas informações de Serviços da AWS log no Amazon S3 — por padrão ou exclusivamente. AWS CloudTrail, Amazon VPC Flow Logs, Elastic Load Balancing, GuardDuty AWS Config Amazon AWS WAF , e são alguns exemplos de serviços que registram informações no Amazon S3. Isso significa que a integridade do log é obtida por meio da integridade do objeto do S3; a confidencialidade do log é obtida por meio dos controles de acesso a objetos do S3; e a disponibilidade do log é obtida por meio do S3 Object Lock, das versões do objeto do S3 e das regras do ciclo de vida do S3.
Ao registrar as informações em um bucket S3 dedicado e centralizado que reside em uma conta dedicada, você pode gerenciar esses registros em apenas alguns buckets e aplicar controles rígidos de segurança, acesso e separação de tarefas.

No AWS SRA, vêm CloudTrail os registros primários armazenados no Amazon S3, portanto, esta seção descreve como proteger esses objetos. Essa orientação também se aplica a qualquer outro objeto do S3 criado por seus próprios aplicativos ou por outros Serviços da AWS. Aplique esses padrões sempre que tiver dados no Amazon S3 que precisem de alta integridade, forte controle de acesso e retenção ou destruição automatizada.

Todos os novos objetos (incluindo CloudTrail registros) que são carregados nos buckets do S3 são criptografados por padrão usando a criptografia do lado do servidor da Amazon com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Isso ajuda a proteger os dados em repouso, mas o controle de acesso é controlado exclusivamente pelas políticas do IAM. Para fornecer uma camada adicional de segurança gerenciada, você pode usar a criptografia do lado do servidor com AWS KMS as chaves que você gerencia (SSE-KMS) em todos os buckets de segurança do S3. Isso adiciona um segundo nível de controle de acesso. Para ler arquivos de log, o usuário deve ter as permissões de leitura do Amazon S3 para o objeto do S3 e uma política ou função do IAM aplicada que permita a decodificação de acordo com a política de chave associada.

Duas opções ajudam você a proteger ou verificar a integridade dos objetos de CloudTrail log armazenados no Amazon S3. CloudTrail fornece validação da integridade do arquivo de log para determinar se um arquivo de log foi modificado ou excluído após a CloudTrail entrega. A outra opção é o S3 Object Lock.

Além de proteger o próprio bucket do S3, você pode seguir o princípio do privilégio mínimo para os serviços de registro (por exemplo, CloudTrail) e a conta do Log Archive. Por exemplo, usuários com permissões concedidas pela política AWS gerenciada do IAM `AWSCloudTrail_FullAccess` podem desativar ou reconfigurar as funções de auditoria mais confidenciais e importantes em suas. Contas da AWS Limite a aplicação dessa política do IAM ao menor número possível de pessoas.

Use controles de detetive, como os fornecidos pelo AWS Config IAM Access Analyzer, para monitorar (alertar e remediar) esse coletivo mais amplo de controles preventivos para mudanças inesperadas.

Para uma discussão mais aprofundada sobre as melhores práticas de segurança para buckets do S3, consulte a documentação do Amazon S3, as palestras técnicas on-line e a postagem do blog As 10 melhores práticas de segurança para proteger dados no Amazon S3.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação do acesso público à conta de bloco do Amazon S3. Esse módulo bloqueia o acesso público do Amazon S3 para todas as contas existentes e futuras na AWS organização.

Amazon Security Lake

AWS A SRA recomenda que você use a conta do Log Archive como a conta de administrador delegado do Amazon Security Lake. Quando você faz isso, o Security Lake coleta registros compatíveis em buckets S3 dedicados na mesma conta que outros registros de segurança recomendados pela SRA.

Para proteger a disponibilidade dos registros e do processo de gerenciamento de registros, os buckets S3 do Security Lake devem ser acessados somente pelo serviço Security Lake ou pelas funções do IAM gerenciadas pelo Security Lake para fontes ou assinantes. Além de usar controles preventivos, como atribuir funções de menor privilégio para acesso e criptografar registros com uma AWS KMS chave controlada, use controles de detetive para monitorar (alertar e corrigir) esse conjunto de permissões em caso de alterações inesperadas. AWS Config

O administrador do Security Lake pode habilitar a coleta de registros em toda a sua AWS organização. Esses registros são armazenados em buckets regionais do S3 na conta do Log Archive. Além disso, para centralizar os registros e facilitar o armazenamento e a análise, o administrador do Security Lake pode escolher uma ou mais regiões cumulativas nas quais os registros de todos os buckets regionais do S3 são consolidados e armazenados. Os registros suportados Serviços da AWS são automaticamente convertidos em um esquema padronizado de código aberto chamado Open Cybersecurity Schema Framework (OCSF) e salvos no formato Apache Parquet nos buckets do Security Lake S3. Com o suporte do OCSF, o Security Lake normaliza e consolida com eficiência os dados de segurança AWS e de outras fontes de segurança corporativa para criar um repositório unificado e confiável de informações relacionadas à segurança.

O Security Lake pode coletar registros associados a eventos AWS CloudTrail de gerenciamento e eventos de CloudTrail dados para o Amazon S3 e. AWS Lambda Para coletar eventos CloudTrail de gerenciamento no Security Lake, você deve ter pelo menos uma trilha CloudTrail organizacional multirregional que colete eventos de CloudTrail gerenciamento de leitura e gravação. O registro de log deve estar habilitado para a trilha. Uma trilha multirregional entrega arquivos de log de várias

regiões para um único bucket S3 para uma única. Conta da AWS Se as regiões estiverem em países diferentes, considere os requisitos de exportação de dados para determinar se as trilhas multirregionais podem ser habilitadas.

AWS Security Hub CSPM é uma fonte de dados nativa compatível com o Security Lake, e você deve adicionar as descobertas do CSPM do Security Hub ao Security Lake. O Security Hub CSPM gera descobertas de várias integrações diferentes Serviços da AWS e de terceiros. Essas descobertas ajudam você a ter uma visão geral de sua postura de conformidade e se você está seguindo as recomendações AWS e AWS Partner soluções de segurança.

Para obter visibilidade e insights acionáveis de registros e eventos, você pode consultar os dados usando ferramentas como Amazon Athena, Amazon Service, OpenSearch Amazon Quick e soluções de terceiros. Os usuários que precisam acessar os dados de log do Security Lake não devem acessar diretamente a conta do Log Archive. Eles devem acessar os dados somente da conta do Security Tooling. Ou eles podem usar outros locais Contas da AWS ou locais que fornecem ferramentas de análise, como OpenSearch Service, Quick, ou ferramentas de terceiros, como ferramentas de gerenciamento de eventos e informações de segurança (SIEM). Para fornecer acesso aos dados, o administrador deve configurar os assinantes do Security Lake na conta do Log Archive e configurar a conta que precisa acessar os dados como assinante de acesso a consultas. Para obter mais informações, consulte Amazon Security Lake na seção Security OU – Security Tooling account deste guia.

O Security Lake fornece uma política AWS gerenciada para ajudá-lo a gerenciar o acesso do administrador ao serviço. Para obter mais informações, consulte o Guia do usuário do Security Lake. Como prática recomendada, recomendamos que você restrinja a configuração do Security Lake por meio de pipelines de desenvolvimento e evite alterações na configuração por meio dos AWS consoles ou do AWS Command Line Interface ()AWS CLI. Além disso, você deve configurar políticas rígidas de IAM e políticas de controle de serviço (SCPs) para fornecer somente as permissões necessárias para gerenciar o Security Lake. Você pode configurar notificações para detectar qualquer acesso direto a esses buckets do S3.

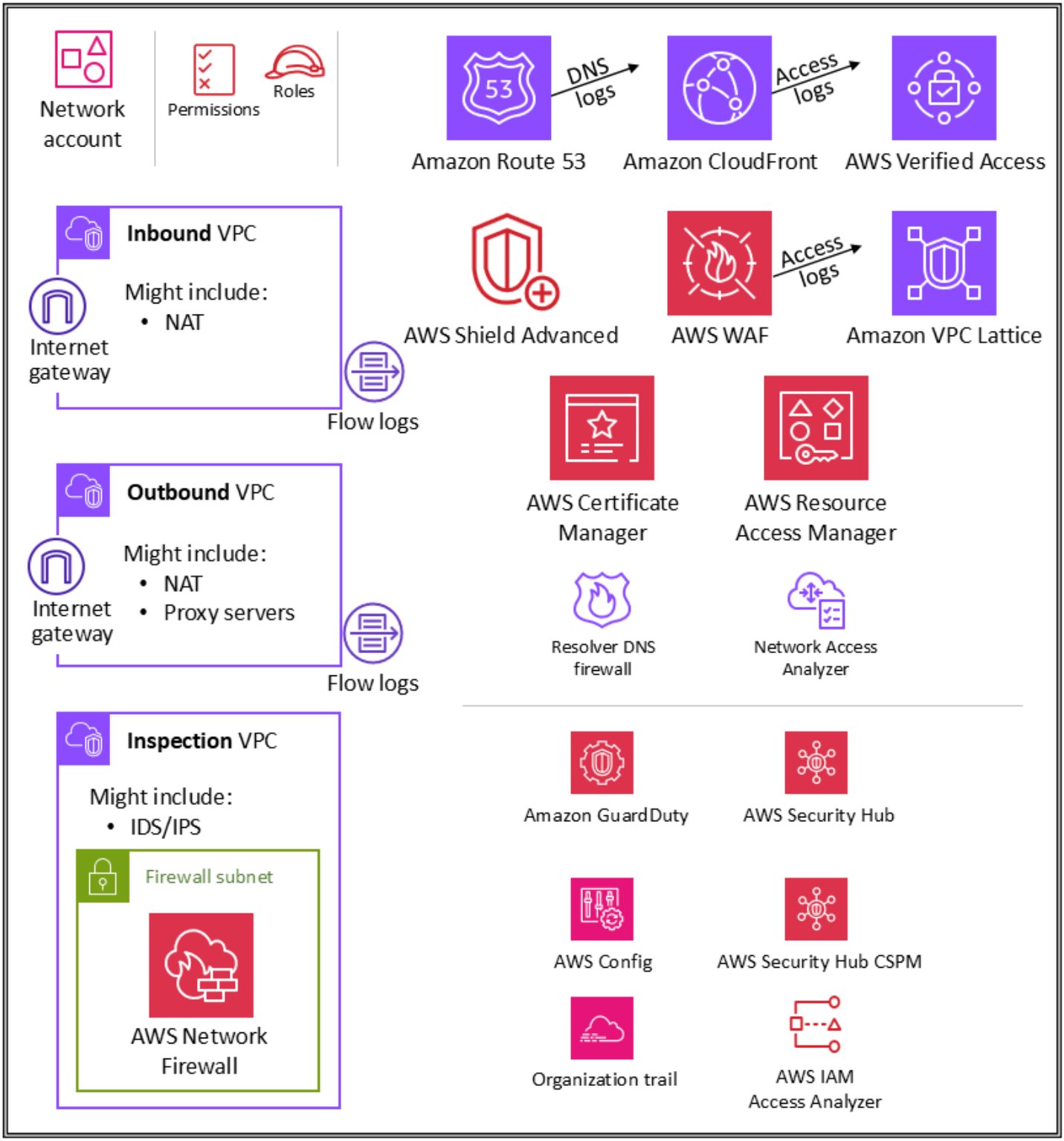
> **Considerações sobre design**
>
> Quando você ativa eventos CloudTrail de gerenciamento no Security Lake, eles resultam em cobranças do Security Lake. A coleção de eventos de CloudTrail gerenciamento no Security Lake exige uma trilha CloudTrail organizacional multirregional que colete eventos de CloudTrail gerenciamento de leitura e gravação. Esta primeira trilha está disponível sem nenhum custo para você. CloudTrail os eventos de gerenciamento normalmente representam

uma pequena porcentagem (cerca de 5%) do total de CloudTrail eventos. Isso se aplica aos clientes que usam AWS Control Tower ou têm CloudTrail registros centralizados em uma conta do Log Archive.

Infraestrutura de UO: conta de Rede

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços de AWS segurança configurados na conta de rede.



A conta de Rede gerencia o gateway entre sua aplicação e a Internet em geral. É importante proteger essa interface bidirecional. A conta de Rede isola os serviços de rede, a configuração e a operação em relação às workloads de aplicações individuais, à segurança e a outras infraestruturas.

Essa disposição não só limita a conectividade, as permissões e o fluxo de dados, mas também possibilita a separação de obrigações e o uso de privilégio mínimo para as equipes que precisem operar nessas contas. Ao dividir o fluxo da rede em nuvens privadas virtuais de entrada e saída (VPCs) separadas, você pode proteger a infraestrutura e o tráfego confidenciais contra acessos indesejados. Em geral, a rede de entrada é considerada de maior risco e merece roteamento, monitoramento e possíveis mitigações de problemas. Essas contas de infraestrutura herdarão as barreiras de proteção de permissão da conta de Gerenciamento da organização e da infraestrutura de unidade organizacional (UO). As equipes de rede (e segurança) gerenciam a maior parte da infraestrutura dessa conta.

Arquitetura de rede

Embora o design e as especificidades da rede estejam além do escopo deste documento, recomendamos essas três opções para conectividade de rede entre as várias contas: emparelhamento AWS PrivateLink de VPC e. AWS Transit Gateway Os fatores importantes ao escolher entre elas são normas operacionais, orçamentos e necessidades específicas de largura de banda.

- Peering de VPC – A maneira mais simples de conectar dois VPCs é usar o peering de VPC. Uma conexão permite a conectividade bidirecional total entre o. VPCs VPCs que estão em contas separadas e também Regiões da AWS podem ser comparadas. Em grande escala, quando você tem dezenas a centenas de VPCs, interconectá-las com o peering resulta em uma malha de centenas a milhares de conexões de peering, o que pode ser difícil de gerenciar e escalar. O emparelhamento de VPC é melhor usado quando os recursos em uma VPC precisam se comunicar com os recursos em outra VPC, o ambiente de ambas VPCs é controlado e protegido e o número de VPCs pessoas conectadas é menor que 10 (para permitir o gerenciamento individual de cada conexão).
- AWS PrivateLink– PrivateLink fornece conectividade privada entre VPCs serviços e aplicativos. Você pode criar seu próprio aplicativo em sua VPC e configurá-lo como um serviço baseado em PrivateLink tecnologia (conhecido como serviço de endpoint). Outros AWS diretores podem criar uma conexão da VPC com seu serviço de endpoint usando uma interface VPC endpoint ou um endpoint Gateway Load Balancer, dependendo do tipo de serviço. Quando você usa PrivateLink, o tráfego do serviço não passa por uma rede pública roteável. Use PrivateLink quando você tiver uma configuração cliente-servidor em que deseja dar a um ou mais consumidores acesso VPCs unidirecional a um serviço específico ou conjunto de instâncias na VPC do provedor de serviços. Essa também é uma boa opção quando clientes e servidores nos dois VPCs têm endereços IP

sobrepostos, porque PrivateLink usa interfaces de rede elásticas na VPC do cliente para que não haja conflitos de IP com o provedor de serviços.

- AWS Transit Gateway– O Transit Gateway fornece um hub-and-spoke design para redes conectadas VPCs e locais como um serviço totalmente gerenciado, sem exigir que você provisione dispositivos virtuais. AWS gerencia alta disponibilidade e escalabilidade. Um gateway de trânsito é um recurso regional e pode conectar milhares de pessoas VPCs dentro do mesmo Região da AWS. Você pode conectar sua conectividade híbrida (VPN e AWS Direct Connect conexões) a um único gateway de trânsito, consolidando e controlando toda a configuração de roteamento da sua AWS organização em um só lugar. Um gateway de trânsito soluciona a complexidade envolvida na criação e no gerenciamento de várias conexões de emparelhamento de VPC em grande escala. É o padrão para a maioria das arquiteturas de rede. No entanto, requisitos específicos de custo, largura de banda e latência podem tornar o emparelhamento de VPC mais adequado às suas necessidades.

VPC de entrada (ingresso)

A VPC de entrada tem como objetivo aceitar, inspecionar e rotear conexões de rede iniciadas de fora do aplicativo. Dependendo dos detalhes específicos da aplicação, você pode esperar ver alguma conversão de endereços de rede (NAT) nessa VPC. Os registros de fluxo dessa VPC serão capturados e armazenados na conta do arquivo de logs.

VPC de saída (egresso)

A VPC de saída é destinada a processar conexões de rede iniciadas diretamente na aplicação. Dependendo das especificidades do aplicativo, você pode esperar ver NAT de tráfego, endpoints de VPC AWS service (Serviço da AWS) específicos e hospedagem de endpoints de API externos nessa VPC. Os registros de fluxo dessa VPC serão capturados e armazenados na conta do arquivo de logs.

VPC de inspeção

Uma VPC de inspeção dedicada fornece uma abordagem simplificada e central para gerenciar inspeções entre VPCs (na mesma ou em diferentes Regiões da AWS) a Internet e as redes locais. Para a AWS SRA, certifique-se de que todo o tráfego entre elas VPCs passe pela VPC de inspeção e evite usar a VPC de inspeção para qualquer outra carga de trabalho.

AWS Network Firewall

AWS Network Firewallé um serviço de firewall de rede gerenciado e altamente disponível para sua VPC. Ele permite que você implante e gerencie facilmente a inspeção monitorada, a prevenção e a detecção de intrusões e a filtragem da web para ajudar a proteger suas redes virtuais. AWS Você pode usar o Network Firewall para descriptografar sessões TLS e inspecionar o tráfego de entrada e saída. Para obter mais informações sobre como configurar o Firewall de Rede, consulte a postagem do AWS Network Firewall blog — Novo serviço gerenciado de firewall na VPC.

Você usa um firewall por zona de disponibilidade em sua VPC. Para cada zona de disponibilidade, você escolhe uma sub-rede para hospedar o endpoint do firewall que filtra seu tráfego. O endpoint do firewall em uma zona de disponibilidade pode proteger todas as sub-redes nessa zona, exceto a sub-rede na qual esteja localizado. A sub-rede do firewall pode ser pública ou privada, dependendo do caso de uso e do modelo de implantação. O firewall é completamente transparente para o fluxo de tráfego e não realiza a conversão de endereços de rede (NAT). Ele preserva os endereços de origem e de destino. Nessa arquitetura de referência, os endpoints do firewall são hospedados em uma VPC de inspeção. Todo o tráfego da VPC de entrada e para a VPC de saída é roteado por essa sub-rede do firewall para inspeção.

O Network Firewall torna a atividade do firewall visível em tempo real por meio das CloudWatch métricas da Amazon e oferece maior visibilidade do tráfego da rede enviando registros para o Amazon Simple Storage Service (Amazon S3) e o Amazon CloudWatch Data Firehose. O Network Firewall é interoperável com sua abordagem de segurança existente, incluindo tecnologias de AWS parceiros. Você também pode importar conjuntos de regras Suricata existentes, que podem ter sido criados internamente ou fornecidos externamente por prestadores terceirizados ou plataformas de código aberto.

No AWS SRA, o Firewall de Rede é usado na conta de rede porque a funcionalidade do serviço focada no controle de rede está alinhada com a intenção da conta.

Considerações sobre design

- AWS Firewall Manager oferece suporte ao Firewall de Rede, para que você possa configurar e implantar centralmente as regras do Firewall de Rede em sua organização. (Para obter detalhes, consulte Usando AWS Network Firewall políticas no Firewall Manager na AWS documentação.) Quando você configura o Firewall Manager, ele cria automaticamente um firewall com conjuntos de regras nas contas e VPCs que

você especifica. Ele também implanta um endpoint em uma sub-rede dedicada para cada zona de disponibilidade que contenha sub-redes públicas. Ao mesmo tempo, todas as alterações no conjunto de regras configurado centralmente são atualizadas automaticamente nos firewalls downstream dos firewalls implantados do Network Firewall.

- O Network Firewall disponibiliza vários modelos de implantação. A abordagem escolhida dependerá do seu caso de uso. Os exemplos incluem:
  - Um modelo de implantação distribuída em que o Network Firewall é implantado individualmente VPCs.
  - Um modelo centralizado de implantação no qual o Network Firewall é implantado em uma VPC centralizada para tráfego no sentido leste/oeste (VPC para VPC) ou no sentido norte/sul (entrada e saída da Internet, on-premises).
  - Um modelo combinado de implantação no qual o Network Firewall é implantado em uma VPC centralizada para tráfego no sentido leste/oeste e em um subconjunto no sentido norte/sul.
- Como prática recomendada, não use a sub-rede do Network Firewall para implantar outros serviços. Isso ocorre porque o Network Firewall não é capaz de inspecionar o tráfego de origens ou destinos na sub-rede do firewall.

Analisador de Acesso à Rede

O Analisador de Acesso à Rede é um recurso da Amazon VPC que identifica acesso de rede inesperado aos seus recursos. Você pode usar o Analisador de Acesso à Rede para validar a segmentação da rede, identificar recursos acessíveis por meio da Internet ou acessíveis exclusivamente a partir de intervalos de endereços IP confiáveis e validar se você tem controles de rede adequados em todos os caminhos de rede.

O Network Access Analyzer usa algoritmos de raciocínio automatizado para analisar os caminhos de rede que um pacote pode percorrer entre os recursos em uma AWS rede e produz descobertas para caminhos que correspondem ao escopo de acesso à rede definido. O Analisador de Acesso à Rede executa uma análise estática de uma configuração de rede, o que significa que nenhum pacote é transmitido na rede como parte dessa análise.

As regras de acessibilidade de rede do Amazon Inspector fornecem um recurso relacionado. As descobertas geradas por essas regras são usadas na conta de Aplicação. Tanto o Network Access Analyzer quanto o Network Reachability usam a tecnologia mais recente da AWS comprovada

iniciativa de segurança e aplicam essa tecnologia em diferentes áreas de foco. O pacote Network Reachability se concentra especificamente nas EC2 instâncias e em sua acessibilidade à Internet.

A conta de rede define a infraestrutura de rede crítica que controla o tráfego que entra e sai do seu AWS ambiente. É necessário monitorar esse tráfego rigorosamente. No AWS SRA, o Network Access Analyzer é usado na conta de rede para ajudar a identificar o acesso não intencional à rede, identificar recursos acessíveis pela Internet por meio de gateways da Internet e verificar se os controles de rede apropriados, como firewalls de rede e gateways NAT, estão presentes em todos os caminhos de rede entre os recursos e os gateways da Internet.

> **Considerações sobre design**
>
> O Network Access Analyzer é um recurso da Amazon VPC e pode ser usado em Conta da AWS qualquer uma que tenha uma VPC. Os administradores de rede podem obter funções de IAM com escopo rigoroso e entre contas para validar se os caminhos de rede aprovados são aplicados em cada uma. Conta da AWS

AWS RAM

AWS Resource Access Manager(AWS RAM) ajuda você a compartilhar com segurança os AWS recursos que você cria em um Conta da AWS com o outro. Contas da AWSAWS RAM fornece um local central para gerenciar o compartilhamento de recursos e padronizar essa experiência em todas as contas. Isso simplifica o gerenciamento de recursos e tira proveito do isolamento administrativo e de cobrança, além de reduzir o escopo dos benefícios de contenção de impacto fornecidos por uma estratégia de várias contas. Se sua conta for gerenciada por AWS Organizations, AWS RAM permite que você compartilhe recursos com todas as contas da organização ou somente com as contas em uma ou mais unidades organizacionais especificadas (OUs). Você também pode compartilhar com um ID Contas da AWS de conta específico, independentemente de a conta fazer parte de uma organização. Você também pode compartilhar alguns tipos de recursos compatíveis com perfis e usuários do IAM especificados.

AWS RAM permite que você compartilhe recursos que não oferecem suporte a políticas baseadas em recursos do IAM, como sub-redes VPC e regras do Route 53. Além disso, com AWS RAM, os proprietários de um recurso podem ver quais diretores têm acesso aos recursos individuais que eles compartilharam. Os diretores do IAM podem recuperar a lista de recursos compartilhados diretamente com eles, o que eles não podem fazer com os recursos compartilhados pelas políticas de recursos do IAM. Se AWS RAM for usado para compartilhar recursos fora da sua AWS

organização, um processo de convite será iniciado. O destinatário deve aceitar o convite antes que o acesso aos recursos seja concedido. Isso fornece freios e contrapesos adicionais.

AWS RAM é invocado e gerenciado pelo proprietário do recurso, na conta em que o recurso compartilhado é implantado. Um caso de uso comum AWS RAM ilustrado na AWS SRA é que os administradores de rede compartilhem sub-redes VPC e gateways de trânsito com toda a organização. AWS Isso fornece a capacidade de desacoplar as funções de gerenciamento de rede Conta da AWS e ajuda a alcançar a separação de tarefas. Para obter mais informações sobre o compartilhamento de VPC, consulte a AWS postagem do blog Compartilhamento de VPC: uma nova abordagem para várias contas e gerenciamento de VPC e o whitepaper de infraestrutura de rede.AWS

> **Considerações sobre design**
>
> Embora AWS RAM o serviço seja implantado somente na conta de rede no AWS SRA, ele normalmente seria implantado em mais de uma conta. Por exemplo, você pode centralizar o gerenciamento do data lake em uma única conta do data lake e depois compartilhar os recursos do catálogo de AWS Lake Formation dados (bancos de dados e tabelas) com outras contas na sua AWS organização. Para obter mais informações, consulte a AWS Lake Formation documentação e a postagem do AWS blog Compartilhe seus dados com segurança entre Contas da AWS os usuários. AWS Lake Formation Além disso, os administradores de segurança podem usar AWS RAM para seguir as melhores práticas ao criar uma Autoridade de Certificação Privada da AWS hierarquia. CAs podem ser compartilhados com terceiros externos, que podem emitir certificados sem ter acesso à hierarquia da CA. Isso permite que as organizações de originação limitem e revoguem o acesso de terceiros.

Acesso Verificado pela AWS

Acesso Verificado pela AWSfornece acesso seguro a aplicativos e recursos corporativos sem uma VPN. Ele melhora a postura de segurança e ajuda a aplicar o acesso de confiança zero avaliando cada solicitação de acesso em tempo real em relação aos requisitos predefinidos. É possível definir uma política de acesso exclusiva para cada aplicação com condições baseadas nos dados de identidade e na postura do dispositivo. O Acesso Verificado fornece acesso seguro a aplicativos HTTP (S), como aplicativos baseados em navegador, e aplicativos não HTTP (S) por meio de protocolos TCP, SSH e RDP para aplicativos como repositórios Git, bancos de dados e grupos de

instâncias. EC2 Eles podem ser acessados usando um terminal de linha de comando ou de um aplicativo de desktop. O Acesso Verificado também simplifica as operações de segurança, ajudando os administradores a definir e monitorar com eficiência as políticas de acesso. Isso deixa mais tempo livre para atualizar políticas, responder a incidentes de segurança e conectividade e auditar os padrões de conformidade. O Verified Access também oferece suporte AWS WAF à integração para ajudá-lo a filtrar ameaças comuns, como injeção de SQL e scripts entre sites (XSS). O Verified Access é perfeitamente integrado ao Centro de Identidade do AWS IAM, o que permite que os usuários se autentiquem com provedores de identidade terceirizados baseados em SAML (). IdPs Se você já tiver uma solução personalizada de IdP compatível com o OpenID Connect (OIDC), o Acesso Verificado também poderá autenticar usuários mediante conexão direta com seu IdP. O Acesso Verificado registra em log todas as tentativas de acesso, permitindo que você responda rapidamente a incidentes de segurança e solicitações de auditoria. O Verified Access suporta a entrega desses registros para o Amazon Simple Storage Service (Amazon S3), Amazon Logs e CloudWatch Amazon Data Firehose.

O Acesso Verificado é compatível com dois padrões comuns de aplicações corporativas: internas e voltadas para a Internet. O Acesso Verificado se integra às aplicações usando Application Load Balancers ou interfaces de rede elástica. Se você estiver usando um Application Load Balancer, o Verified Access requer um balanceador de carga interno. Como o Verified Access oferece suporte AWS WAF no nível da instância, um aplicativo existente que tenha AWS WAF integração com um Application Load Balancer pode mover políticas do balanceador de carga para a instância do Verified Access. Um aplicação corporativa é representada como um endpoint do Acesso Verificado. Cada endpoint está associado a um grupo de Acesso Verificado e herda a política de acesso do grupo. Um grupo do Acesso Verificado é uma coleção de endpoints do Acesso Verificado e uma política do Acesso Verificado no nível de grupo. Os grupos simplificam o gerenciamento de políticas e permitem que os administradores de TI definam critérios básicos. Os proprietários da aplicação podem definir ainda mais políticas granulares de acordo com a sensibilidade da aplicação.

No AWS SRA, o acesso verificado é hospedado na conta de rede. A equipe central de TI define centralmente as configurações gerenciadas. Por exemplo, a equipe pode conectar provedores de confiança, como provedores de identidade (por exemplo, Okta) e provedores de confiança de dispositivos (por exemplo, Jamf), criar grupos e determinar a política por grupo. Essas configurações podem então ser compartilhadas com dezenas, centenas ou milhares de contas de carga de trabalho usando. AWS RAM Isso permite que as equipes de aplicativos gerenciem os endpoints subjacentes que gerenciam seus aplicativos sem a sobrecarga de outras equipes. AWS RAM fornece uma maneira escalável de aproveitar o Acesso Verificado para aplicativos corporativos hospedados em diferentes contas de carga de trabalho.

Considerações sobre design

É possível agrupar os endpoints para aplicações com requisitos de segurança semelhantes a fim de simplificar a administração de políticas e então compartilhar com grupo com contas de aplicação. Todas as aplicações do grupo compartilham a política do grupo. Se uma aplicação do grupo exigir uma política específica devido a um caso de borda, você poderá aplicar uma política por aplicação para essa aplicação.

Amazon VPC Lattice

O Amazon VPC Lattice é um serviço de rede de aplicativos que conecta, monitora e protege as comunicações. service-to-service Um serviço, geralmente chamado de microsserviço, é uma unidade de software implantável de forma independente que entrega uma tarefa específica. O VPC Lattice gerencia automaticamente a conectividade de rede e o roteamento da camada de aplicativos entre serviços entre e Contas da AWS sem exigir que você VPCs gerencie a conectividade de rede subjacente, os balanceadores de carga de front-end ou os proxies secundários. O serviço fornece um proxy totalmente gerenciado de camada de aplicação que oferece roteamento por aplicação com base nas características da solicitação, como caminhos e cabeçalhos. O VPC Lattice é incorporado à infraestrutura do VPC, portanto, fornece uma abordagem consistente em uma ampla variedade de tipos de computação, como Amazon Elastic Compute Cloud (Amazon), Amazon EC2 Elastic Kubernetes Service (Amazon EKS) e. AWS Lambda O VPC Lattice também oferece suporte a roteamento ponderado e implantações no estilo canário. blue/green Você pode usar o VPC Lattice para criar uma rede de serviços com um limite lógico que implementa automaticamente a descoberta e a conectividade de serviços. O VPC Lattice se integra ao IAM para service-to-service autenticação e autorização usando políticas de autenticação.

O VPC Lattice se integra AWS RAM para permitir o compartilhamento de serviços e redes de serviços. AWS O SRA descreve uma arquitetura distribuída em que desenvolvedores ou proprietários de serviços criam serviços VPC Lattice em sua conta de aplicativo. Os proprietários do serviço definem os receptores, as regras de roteamento e os grupos de destino juntamente com as políticas de autenticação. Em seguida, eles compartilham os serviços com outras contas e os associam às redes de serviços VPC Lattice. Essas redes são criadas pelos administradores de rede na conta de Rede e compartilhadas com a conta de Aplicação. Os administradores de rede configuram políticas de autenticação e monitoramento para cada rede de serviços. Os administradores associam os VPCs serviços do VPC Lattice a uma ou mais redes de serviços. Para uma explicação detalhada dessa arquitetura distribuída, consulte a postagem do AWS blog Crie

conectividade segura de várias contas e várias VPC para seus aplicativos com o Amazon VPC Lattice

Considerações sobre design

- Dependendo do modelo operacional de serviço ou da visibilidade da rede de serviços da sua organização, os administradores de rede podem compartilhar suas redes de serviços e dar aos proprietários de serviços o controle de associar seus serviços e VPCs a essas redes de serviços. Como alternativa, os proprietários de serviço podem compartilhar seus serviços e os administradores de rede podem associar os serviços às redes de serviços.
- Um cliente só poderá enviar solicitações para serviços associados a uma rede de serviços se o cliente estiver em uma VPC que esteja associada à mesma rede de serviços. O tráfego do cliente que atravessar uma conexão de emparelhamento da VPC ou um gateway de trânsito será negado.

Segurança de borda

A segurança de borda geralmente envolve três tipos de proteções: entrega segura de conteúdo, proteção da rede e da camada de aplicativos e mitigação distribuída de negação de serviço (S). DDo Conteúdos como dados, vídeos, aplicativos e APIs precisam ser entregues com rapidez e segurança, usando a versão recomendada do TLS para criptografar as comunicações entre endpoints. O conteúdo também deve ter restrições de acesso por meio de cookies assinados e assinados e autenticação por token. URLs Deve-se projetar a segurança por aplicação para controlar o tráfego de bots, bloquear padrões de ataque comuns, como injeção de SQL ou cross-site scripting (XSS), e fornecer visibilidade do tráfego na Web. No limite, a mitigação DDo S fornece uma importante camada de defesa que garante a disponibilidade contínua de operações e serviços comerciais essenciais. Os aplicativos APIs devem ser protegidos contra inundações de SYN, inundações de UDP ou outros ataques de reflexão e ter mitigação em linha para impedir ataques básicos na camada de rede.

AWS oferece vários serviços para ajudar a fornecer um ambiente seguro, desde a nuvem central até a borda da AWS rede. A Amazon CloudFront, AWS Certificate Manager (ACM), AWS Shield AWS WAF, e o Amazon Route 53 trabalham juntos para ajudar a criar um perímetro de segurança flexível e em camadas. Com CloudFront APIs, o conteúdo ou os aplicativos podem ser fornecidos por HTTPS usando TLSv1 .3 para criptografar e proteger a comunicação entre clientes visualizadores e. CloudFront Você pode usar o ACM para criar um certificado SSL personalizado e implantá-lo

em uma CloudFront distribuição gratuitamente. O ACM gerencia automaticamente a renovação do certificado. O Shield é um serviço gerenciado de proteção DDo S que ajuda a proteger os aplicativos executados no AWS. Ele fornece detecção dinâmica e mitigações automáticas em linha que minimizam o tempo de inatividade e a latência do aplicativo. AWS WAF permite criar regras para filtrar o tráfego da web com base em condições específicas (endereços IP, cabeçalhos e corpo HTTP ou personalizados URIs), ataques comuns na web e bots generalizados. O Amazon Route 53 é um web service DNS altamente disponível e dimensionável. O Route 53 conecta solicitações de usuários a aplicativos da Internet que são executados no local AWS ou no local. O AWS SRA adota uma arquitetura de entrada de rede centralizada usando AWS Transit Gateway, hospedada na conta de rede, de forma que a infraestrutura de segurança de ponta também esteja centralizada nessa conta.

Amazon CloudFront

CloudFrontA Amazon é uma rede de entrega de conteúdo (CDN) segura que fornece proteção inerente contra tentativas comuns de camada de rede e transporte DDo S. Você pode entregar seu conteúdo ou aplicativos usando certificados TLS, e os recursos avançados de TLS são ativados automaticamente. APIs Você pode usar AWS Certificate Manager (ACM) para criar um certificado TLS personalizado e impor comunicações HTTPS entre visualizadores e CloudFront, conforme descrito posteriormente na seção ACM. Além disso, você pode exigir que as comunicações entre sua origem personalizada CloudFront e sua origem personalizada implementem end-to-end criptografia em trânsito. Para esse cenário, você deverá instalar um certificado TLS no seu servidor de origem. Se sua origem for um balanceador de carga elástico, você poderá usar um certificado gerado pelo ACM ou um certificado validado por uma autoridade de certificação (CA) externa e importado para o ACM. Se os endpoints do site do bucket S3 servirem como origem para CloudFront, você não poderá configurar CloudFront para usar HTTPS com sua origem, porque o Amazon S3 não oferece suporte a HTTPS para endpoints de sites. (No entanto, você ainda pode exigir HTTPS entre os espectadores CloudFront e.) Para todas as outras origens compatíveis com a instalação de certificados HTTPS, será necessário usar um certificado assinado por uma CA externa.

CloudFront fornece várias opções para proteger e restringir o acesso ao seu conteúdo. Por exemplo, ele pode restringir o acesso à sua origem do Amazon S3 usando cookies assinados URLs e assinados. Para obter mais informações, consulte Configurar o acesso seguro e restringir o acesso ao conteúdo na CloudFront documentação.

O AWS SRA ilustra CloudFront as distribuições centralizadas na conta de rede porque elas se alinham ao padrão de rede centralizado que é implementado usando. AWS Transit Gateway Ao implantar e gerenciar CloudFront distribuições na conta de rede, você obtém os benefícios dos controles centralizados. Você pode gerenciar todas as CloudFront distribuições em um único local,

o que facilita o controle do acesso, a configuração das configurações e o monitoramento do uso em todas as contas. Além disso, você pode gerenciar os certificados ACM, os registros DNS e o CloudFront registro em uma conta centralizada.

O painel CloudFront de segurança fornece AWS WAF visibilidade e controles diretamente em sua CloudFront distribuição. Você obtém visibilidade das principais tendências de segurança do seu aplicativo, do tráfego permitido e bloqueado e da atividade de bots. Você pode usar ferramentas investigativas, como analisadores visuais de registros e controles de bloqueio integrados, para isolar padrões de tráfego e bloquear o tráfego sem consultar registros ou escrever regras de segurança.

Considerações sobre design

- Como alternativa, você pode implantar CloudFront como parte do aplicativo na conta do aplicativo. Nesse cenário, a equipe de aplicativos toma decisões como a forma como CloudFront as distribuições são implantadas, determina as políticas de cache apropriadas e assume a responsabilidade pela governança, auditoria e monitoramento das distribuições. CloudFront Ao CloudFront distribuir as distribuições em várias contas, você pode se beneficiar de cotas de serviço adicionais. Como outro benefício, você pode usar a configuração CloudFront de identidade de acesso de origem (OAI) e controle de acesso de origem (OAC) inerente e automatizada para restringir o acesso às origens do Amazon S3.
- Quando você entrega conteúdo da web por meio de uma CDN CloudFront, como, você precisa impedir que os espectadores ignorem a CDN e acessem seu conteúdo de origem diretamente. Para alcançar essa restrição de acesso à origem, você pode usar CloudFront e AWS WAF adicionar cabeçalhos personalizados e verificar os cabeçalhos antes de encaminhar as solicitações para sua origem personalizada. Para obter uma explicação detalhada dessa solução, consulte a postagem do blog de AWS segurança Como aprimorar a segurança de CloudFront origem da Amazon com AWS WAFAWS Secrets Manager e. Um método alternativo é limitar somente a lista de CloudFront prefixos no grupo de segurança associado ao Application Load Balancer. Isso ajudará a garantir que somente uma CloudFront distribuição possa acessar o balanceador de carga.

AWS WAF

AWS WAFé um firewall de aplicativos da Web que ajuda a proteger seus aplicativos da Web contra explorações da Web, como vulnerabilidades comuns e bots, que podem afetar a disponibilidade dos aplicativos, comprometer a segurança ou consumir recursos excessivos. Ele pode ser integrado com

uma CloudFront distribuição da Amazon, uma API REST do Amazon API Gateway, um Application Load Balancer, uma API GraphQL, um AWS AppSync grupo de usuários do Amazon Cognito e o serviço. AWS App Runner

AWS WAF usa listas de controle de acesso à web (ACLs) para proteger um conjunto de AWS recursos. Uma ACL da web é um conjunto de regras que define os critérios de inspeção e uma ação associada a ser tomada (bloquear, permitir, contar ou executar o controle do bot) se uma solicitação da web atender aos critérios. AWS WAF fornece um conjunto de regras gerenciadas que fornece proteção contra vulnerabilidades comuns de aplicativos. Essas regras são organizadas e gerenciadas por AWS AWS nossos parceiros. AWS WAF também oferece uma linguagem de regras poderosa para criar regras personalizadas. É possível usar regras personalizadas para escrever critérios de inspeção que atendam às suas necessidades específicas. Os exemplos incluem restrições de IP, restrições geográficas e versões personalizadas de regras gerenciadas que se adaptem melhor ao comportamento específico da sua aplicação.

AWS WAF fornece um conjunto de regras inteligentes gerenciadas por níveis para bots comuns e direcionados e proteção contra invasão de contas (ATP). Você paga uma tarifa de assinatura e uma tarifa de inspeção de tráfego ao usar os grupos de regras para controle de bots e para ATP. Por isso, recomendamos que você monitore o tráfego antes e então decida o que usar. Você pode usar os painéis de gerenciamento de bots e controle de contas que estão disponíveis gratuitamente no AWS WAF console para monitorar essas atividades e depois decidir se você precisa de um grupo de AWS WAF regras de nível inteligente.

No AWS SRA, AWS WAF está integrado à conta CloudFront de rede. Nessa configuração, o processamento de AWS WAF regras acontece nos pontos de presença em vez de dentro da VPC. Isso permite filtrar o tráfego malicioso mais perto do usuário final que solicitou o conteúdo e ajuda a impedir que o tráfego malicioso entre na sua rede principal.

Você pode enviar AWS WAF registros completos para um bucket do S3 na conta do Log Archive configurando o acesso entre contas ao bucket do S3. Para obter mais informações, consulte o artigo do AWS re:POST sobre esse tópico.

Considerações sobre design

- Como alternativa à implantação AWS WAF centralizada na conta de rede, alguns casos de uso são melhor atendidos com a implantação AWS WAF na conta do aplicativo. Por exemplo, você pode escolher essa opção ao implantar suas CloudFront distribuições em sua conta de aplicativo ou ter balanceadores de carga de aplicativos voltados para o

público ou se estiver usando o API Gateway na frente de seus aplicativos web. Se você decidir implantar AWS WAF em cada conta do aplicativo, use AWS Firewall Manager para gerenciar AWS WAF as regras nessas contas a partir da conta centralizada do Security Tooling.

- Você também pode adicionar AWS WAF regras gerais na CloudFront camada e AWS WAF regras adicionais específicas do aplicativo em um recurso regional, como o Application Load Balancer ou o gateway da API.

AWS Shield

AWS Shieldé um serviço gerenciado de proteção DDo S que protege os aplicativos executados em AWS. Existem dois níveis de Shield: Shield Standard e Shield Advanced. O Shield Standard oferece a todos os AWS clientes proteção contra os eventos de infraestrutura mais comuns (camadas 3 e 4) sem custo adicional. O Shield Advanced fornece mitigações automáticas mais sofisticadas para eventos não autorizados que visam aplicativos em zonas protegidas hospedadas da Amazon EC2, do Elastic Load Balancing (Elastic Load Balancing) e do CloudFront Route AWS Global Accelerator 53. Se você possui sites de alta visibilidade ou está propenso a ataques DDo S frequentes, considere os recursos adicionais que o Shield Advanced oferece.

Você pode usar o recurso de mitigação automática da camada DDo S do aplicativo Shield Advanced para configurar o Shield Advanced para responder automaticamente para mitigar os ataques da camada de aplicação (camada 7) contra suas CloudFront distribuições protegidas, balanceadores de carga do Elastic Load Balancing (Elastic Load Balancing) (aplicativo, rede e clássico), zonas hospedadas do Amazon Route 53, endereços IP do Amazon Elastic e aceleradores padrão. EC2 AWS Global Accelerator Quando você ativa esse recurso, o Shield Advanced gera automaticamente AWS WAF regras personalizadas para mitigar DDo os ataques S. O Shield Advanced também dá acesso à Equipe de AWS Shield Resposta (SRT). Você pode entrar em contato com a SRT a qualquer momento para criar e gerenciar mitigações personalizadas para seu aplicativo ou durante um ataque S ativo DDo. Se você quiser que o SRT monitore proativamente seus recursos protegidos e entre em contato com você durante uma tentativa DDo S, considere ativar o recurso de engajamento proativo.

Considerações sobre design

- Se você tiver alguma carga de trabalho baseada em recursos voltados para a Internet na conta do aplicativo, como um Application Load Balancer ou um Network CloudFront Load

Balancer, configure o Shield Advanced na conta do aplicativo e adicione esses recursos à proteção do Shield. Você pode usar AWS Firewall Manager para configurar essas opções em grande escala.

- Se você tiver vários recursos no fluxo de dados, como uma CloudFront distribuição na frente de um Application Load Balancer, use somente o recurso de ponto de entrada como recurso protegido. Isso garantirá que você não pague as tarifas do Shield Data Transfer Out (DTO – Saída de transferência de dados) duplamente por dois recursos.
- O Shield Advanced registra métricas que você pode monitorar na Amazon CloudWatch. (Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch na AWS documentação.) Configure CloudWatch alarmes para receber notificações do SNS em sua central de segurança quando um evento DDo S for detectado. Em um evento suspeito de DDo S, entre em contato com a equipe do AWS Enterprise Support preenchendo um ticket de suporte e atribuindo a ele a maior prioridade. A equipe do Enterprise Support incluirá a Shield Response Team (SRT) ao processar o evento. Além disso, você pode pré-configurar a função Lambda de AWS Shield engajamento para criar um ticket de suporte e enviar um e-mail para a equipe do SRT.

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) permite provisionar, gerenciar e implantar certificados TLS públicos e privados para uso com seus Serviços da AWS recursos internos conectados. Com o ACM, você pode solicitar rapidamente um certificado, implantá-lo em AWS recursos integrados ao ACM, como balanceadores de carga do Elastic Load Balancing, distribuições e no Amazon APIs API Gateway CloudFront , e deixar que o ACM cuide das renovações de certificados. Quando você solicita certificados públicos do ACM, não há necessidade de gerar um key pair ou uma solicitação de assinatura de certificado (CSR), enviar uma CSR a uma autoridade de certificação (CA) ou carregar e instalar o certificado quando ele for recebido. O ACM também oferece a opção de importar certificados TLS emitidos por terceiros CAs e implantá-los com os serviços integrados do ACM. Quando você opta por gerenciar certificados com o ACM, as chaves privadas são protegidas e armazenadas de maneira segura, seguindo as melhores práticas de criptografia e gestão de chaves. Com o ACM, não há cobrança adicional pelo provisionamento de certificados públicos, e o ACM gerencia o processo de renovação.

O ACM é usado na conta de rede para gerar um certificado TLS público, que, por sua vez, é usado pelas CloudFront distribuições para estabelecer a conexão HTTPS entre visualizadores e. CloudFront Para obter mais informações, consulte a documentação do CloudFront .

> **Considerações sobre design**
>
> Para certificados direcionados externamente, o ACM deverá residir na mesma conta dos recursos para os quais ele fornece certificados. Não é possível compartilhar certificados entre contas.

Amazon Route 53

O Amazon Route 53 é um serviço web de DNS altamente disponível e escalável. Você pode usar o Route 53 para executar três funções principais: registro de domínios, roteamento de DNS e verificação de integridade.

Você pode usar o Route 53 como um serviço de DNS para mapear nomes de domínio para suas EC2 instâncias, buckets S3, CloudFront distribuições e outros recursos. AWS A natureza distribuída dos servidores AWS DNS ajuda a garantir que seus usuários finais sejam roteados para seu aplicativo de forma consistente. Recursos como fluxo de tráfego e controle de roteamento do Route 53 ajudam você a melhorar a confiabilidade. Se o endpoint principal de aplicação ficar indisponível, você poderá configurar seu failover para redirecionar seus usuários para um local alternativo. O Route 53 Resolver fornece DNS recursivo para sua VPC e redes locais por meio de uma VPN gerenciada. AWS Direct Connect AWS

Ao usar o serviço IAM com o Route 53, você obtém um controle refinado sobre quem pode atualizar seus dados de DNS. É possível habilitar a assinatura Domain Name System Security Extensions (DNSSEC) para permitir que os resolvedores de DNS validem que uma resposta de DNS veio do Route 53 e não foi adulterada.

O Route 53 Resolver DNS Firewall fornece proteção para solicitações de DNS de saída do seu. VPCs Essas solicitações passam pelo Route 53 Resolver para resolução de nomes de domínio. Um uso principal das proteções do Firewall DNS é ajudar a impedir a exfiltração de DNS de seus dados. Com o Firewall DNS, você pode monitorar e controlar os domínios que as aplicações podem consultar. Você pode negar acesso aos domínios sabidamente nocivos e permitir a passagem de todas as outras consultas. Como alternativa, você pode negar acesso a todos os domínios, exceto aqueles em que você confia explicitamente. Você também pode usar o DNS Firewall para bloquear

solicitações de resolução para recursos em zonas hospedadas privadas (compartilhadas ou locais), incluindo nomes de endpoint da VPC. Ele também pode bloquear solicitações de nomes de EC2 instâncias públicas ou privadas.

Os resolvedores do Route 53 são criados por padrão como parte de cada VPC. No AWS SRA, o Route 53 é usado na conta de rede principalmente para o recurso de firewall DNS.

Considerações sobre design

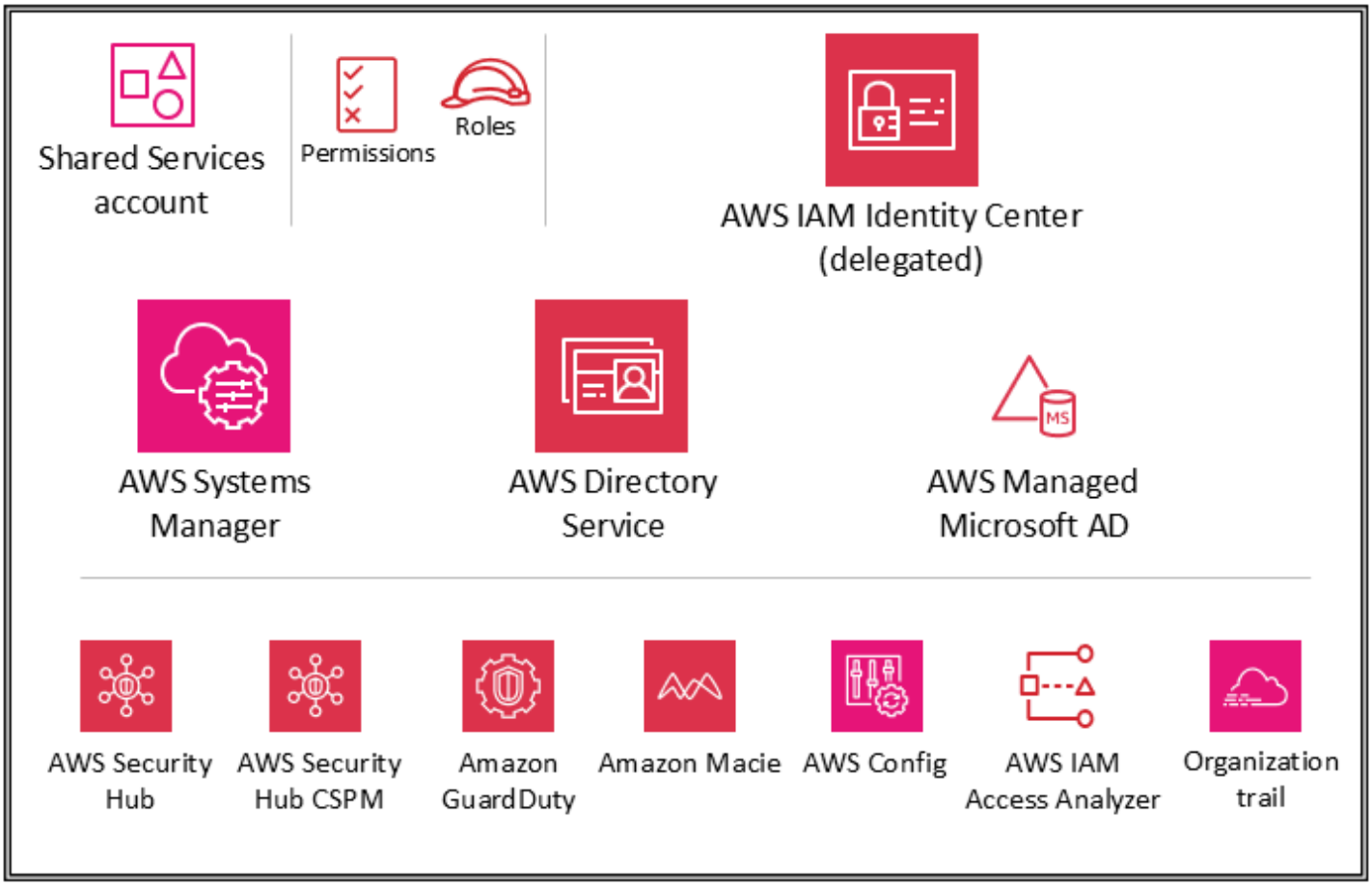
O DNS Firewall e AWS Network Firewall ambos oferecem filtragem de nomes de domínio, mas para diferentes tipos de tráfego. Você pode usar o Firewall DNS e o Firewall de Rede juntos para configurar a filtragem baseada em domínio para o tráfego da camada de aplicativo em dois caminhos de rede diferentes:

- O Firewall DNS fornece filtragem para consultas DNS de saída que passam pelo Resolvedor do Route 53 a partir de aplicativos dentro do seu. VPCs Você também pode configurar o Firewall DNS para enviar respostas personalizadas para consultas a nomes de domínio bloqueados.
- O Network Firewall fornece filtragem para tráfego de camada de rede e camada de aplicação, mas não tem visibilidade sobre as consultas feitas pelo Route 53 Resolver.

Infraestrutura OU — conta de serviços compartilhados

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços AWS de segurança configurados na conta do Shared Services.



A conta de Serviços Compartilhados faz parte da UO de Infraestrutura e seu objetivo é oferecer suporte aos serviços que vários aplicativos e equipes usam para fornecer seus resultados. Por exemplo, serviços de diretório (Active Directory), serviços de mensagens e serviços de metadados estão nessa categoria. O AWS SRA destaca os serviços compartilhados que oferecem suporte aos controles de segurança. Embora as contas de rede também façam parte da OU de infraestrutura, elas são removidas da conta de Serviços Compartilhados para apoiar a separação de tarefas. As equipes que gerenciarão esses serviços não precisam de permissões ou acesso às contas da Rede.

AWS Systems Manager

AWS Systems Manager(que também está incluída na conta de gerenciamento da organização e na conta do aplicativo) fornece um conjunto de recursos que permitem a visibilidade e o controle de seus AWS recursos. Um desses recursos, o Systems Manager Explorer, é um painel de operações personalizável que relata informações sobre seus AWS recursos. Você pode sincronizar dados de operações em todas as contas em sua AWS organização usando o AWS Organizations Systems

Manager Explorer. O Systems Manager é implantado na conta do Shared Services por meio da funcionalidade de administrador delegado em. AWS Organizations

O Systems Manager ajuda você a trabalhar para manter a segurança e a conformidade examinando suas instâncias gerenciadas e relatando (ou tomando medidas corretivas) sobre quaisquer violações de políticas detectadas. Ao combinar o Systems Manager com implantações apropriadas em cada membro Contas da AWS (por exemplo, a conta do aplicativo), você pode coordenar a coleta de dados de inventário de instâncias e centralizar a automação, como atualizações de segurança e patches.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD, permite que suas cargas de trabalho e AWS recursos com reconhecimento de diretório usem o Active Directory gerenciado em. AWS Você pode usar AWS Managed Microsoft AD para unir instâncias do Amazon EC2 para Windows Server, Amazon EC2 para Linux e Amazon RDS for SQL Server ao seu domínio e AWS usar serviços de computação de usuário final (EUC), como a WorkSpacesAmazon, com usuários e grupos do Active Directory.

AWS Managed Microsoft AD ajuda você a estender seu Active Directory existente AWS e usar suas credenciais de usuário locais existentes para acessar recursos na nuvem. Você também pode administrar seus usuários, grupos, aplicativos e sistemas locais sem a complexidade de executar e manter um Active Directory local e altamente disponível. Você pode unir seus computadores, laptops e impressoras existentes a um AWS Managed Microsoft AD domínio.

AWS Managed Microsoft AD é construído no Microsoft Active Directory e não exige que você sincronize ou replique dados do seu Active Directory existente para a nuvem. Você pode usar ferramentas e recursos de administração conhecidos do Active Directory, como Objetos de Política de Grupo (GPOs), relações de confiança de domínio, políticas de senha refinadas, Contas de Serviços Gerenciados (gMSAs) de grupo, extensões de esquema e login único baseado em Kerberos. Você também pode delegar tarefas administrativas e autorizar o acesso usando grupos de segurança do Active Directory.

A replicação multirregional permite que você implante e use um único AWS Managed Microsoft AD diretório em vários. Regiões da AWS Isso torna mais fácil e econômico implantar e gerenciar suas cargas de trabalho do Microsoft Windows e Linux globalmente. Ao usar o recurso automatizado de replicação multirregional, você obtém maior resiliência enquanto seus aplicativos usam um diretório local para um desempenho ideal.

AWS Managed Microsoft AD oferece suporte ao Lightweight Directory Access Protocol (LDAP) sobre SSL/TLS, também conhecido como LDAPS, nas funções de cliente e servidor. Ao atuar como servidor, AWS Managed Microsoft AD oferece suporte a LDAPS nas portas 636 (SSL) e 389 (TLS). Você habilita as comunicações LDAPS do lado do servidor instalando um certificado em seus controladores de AWS Managed Microsoft AD domínio a partir de uma autoridade de certificação (CA) AWS baseada nos Serviços de Certificados do Active Directory (AD CS). Ao atuar como cliente, AWS Managed Microsoft AD oferece suporte a LDAPS nas portas 636 (SSL). Você pode habilitar as comunicações LDAPS do lado do cliente registrando os certificados CA dos emissores de certificados do servidor e AWS, em seguida, habilitando o LDAPS em seu diretório.

No AWS SRA, Directory Service é usado na conta do Shared Services para fornecer serviços de domínio para cargas de trabalho compatíveis com a Microsoft em várias contas de membros. AWS

> **Considerações sobre design**
>
> Você pode conceder aos usuários locais do Active Directory acesso para entrar no Console de gerenciamento da AWS and AWS Command Line Interface (AWS CLI) com suas credenciais existentes do Active Directory usando o IAM Identity Center e selecionando AWS Managed Microsoft AD como fonte de identidade. Isso permite que seus usuários assumam uma das funções atribuídas no login e acessem e ajam nos recursos de acordo com as permissões definidas para a função. Uma opção alternativa é usar para AWS Managed Microsoft AD permitir que seus usuários assumam uma função do IAM.

Centro de Identidade do IAM

O AWS SRA usa o recurso de administrador delegado suportado por Centro de Identidade do AWS IAM para delegar a maior parte da administração do IAM Identity Center à conta do Shared Services. Isso ajuda a restringir o número de usuários que precisam de acesso à conta de gerenciamento da organização. O IAM Identity Center ainda precisa ser ativado na conta de gerenciamento da organização para realizar determinadas tarefas, incluindo o gerenciamento de conjuntos de permissões provisionados na conta de gerenciamento da organização.

O principal motivo para usar a conta do Shared Services como administrador delegado do IAM Identity Center é a localização do Active Directory. Se você planeja usar o Active Directory como sua fonte de identidade do IAM Identity Center, precisará localizar o diretório na conta do membro que você designou como sua conta de administrador delegado do IAM Identity Center. No AWS SRA, a

conta do Shared Services hospeda AWS Managed Microsoft AD, de modo que essa conta se torne a administradora delegada do IAM Identity Center.

O IAM Identity Center suporta o registro de uma única conta de membro como administrador delegado ao mesmo tempo. Você pode registrar uma conta de membro somente quando fizer login com as credenciais da conta de gerenciamento. Para habilitar a delegação, você precisa considerar os pré-requisitos listados na documentação do IAM Identity Center. A conta de administrador delegado pode realizar a maioria das tarefas de gerenciamento do IAM Identity Center, mas com algumas restrições, que estão listadas na documentação do IAM Identity Center. O acesso à conta de administrador delegado do IAM Identity Center deve ser rigorosamente controlado.

Considerações sobre design

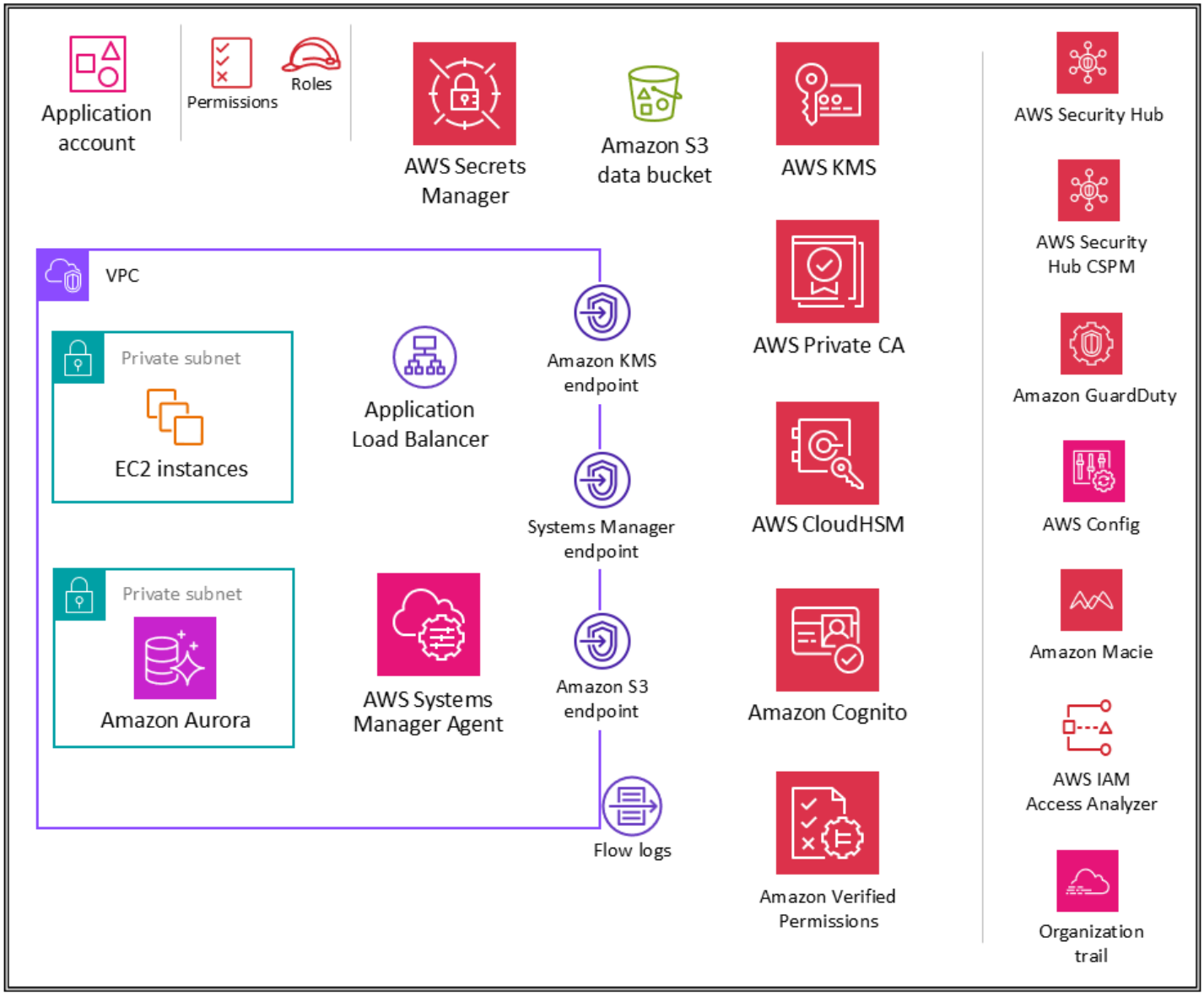
- Se você decidir alterar a fonte de identidade do IAM Identity Center de qualquer outra fonte para o Active Directory, ou alterá-la do Active Directory para qualquer outra fonte, o diretório deverá residir (pertencer à) conta de membro do administrador delegado do IAM Identity Center, se houver; caso contrário, deverá estar na conta de gerenciamento.
- Você pode hospedar sua AWS Managed Microsoft AD em uma VPC dedicada em uma conta diferente e depois usar AWS Resource Access Manager (AWS RAM) para compartilhar sub-redes dessa outra conta com a conta de administrador delegado. Dessa forma, a AWS Managed Microsoft AD instância é controlada na conta do administrador delegado, mas, do ponto de vista da rede, ela age como se estivesse implantada na VPC de outra conta. Isso é útil quando você tem várias AWS Managed Microsoft AD instâncias e deseja implantá-las localmente onde sua carga de trabalho está sendo executada, mas gerenciá-las centralmente por meio de uma conta.
- Se você tem uma equipe de identidade dedicada que realiza atividades regulares de gerenciamento de identidade e acesso ou tem requisitos rígidos de segurança para separar as funções de gerenciamento de identidade de outras funções de serviços compartilhados, você pode hospedar uma dedicada Conta da AWS para gerenciamento de identidade. Nesse cenário, você designa essa conta como administrador delegado do IAM Identity Center e ela também hospeda seu AWS Managed Microsoft AD diretório. Você pode alcançar o mesmo nível de isolamento lógico entre suas cargas de trabalho de gerenciamento de identidade e outras cargas de trabalho de serviços compartilhados usando permissões refinadas do IAM em uma única conta de serviço compartilhado.
- Atualmente, o IAM Identity Center não oferece suporte a várias regiões. (Para habilitar o IAM Identity Center em uma região diferente, você deve primeiro excluir a configuração

atual do IAM Identity Center.) Além disso, ele não suporta o uso de diferentes fontes de identidade para diferentes conjuntos de contas nem permite que você delegue o gerenciamento de permissões a diferentes partes da sua organização (ou seja, vários administradores delegados) ou a diferentes grupos de administradores. Se você precisar de algum desses recursos, poderá usar a federação do IAM para gerenciar suas identidades de usuário dentro de um provedor de identidade (IdP) externo e dar permissão a essas identidades AWS de usuário externo para AWS usar recursos em sua conta. Suportes do IdPs IAM compatíveis com OpenID Connect (OIDC) ou SAML 2.0. Como prática recomendada, use a federação SAML 2.0 com provedores de identidade terceirizados, como Active Directory Federation Service (AD FS), Okta, Azure Active Directory (Azure AD) ou Ping Identity para fornecer capacidade de login único para que os usuários façam login Console de gerenciamento da AWS ou chamem operações de API. AWS Para obter mais informações sobre federação e provedores de identidade do IAM, consulte Sobre a federação baseada no SAML 2.0 na documentação do IAM.

Workloads OU — Conta de aplicativo

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços de AWS segurança configurados na conta do aplicativo (junto com o próprio aplicativo).



A conta do aplicativo hospeda a infraestrutura e os serviços principais para executar e manter um aplicativo corporativo. A conta do aplicativo e a UO de cargas de trabalho atendem a alguns objetivos principais de segurança. Primeiro, você cria uma conta separada para cada aplicativo para fornecer limites e controles entre cargas de trabalho para evitar problemas de combinação de funções, permissões, dados e chaves de criptografia. Você deseja fornecer um contêiner de conta separado, no qual a equipe de aplicativos possa ter amplos direitos para gerenciar sua própria infraestrutura sem afetar outras pessoas. Em seguida, você adiciona uma camada de proteção fornecendo um mecanismo para a equipe de operações de segurança monitorar e coletar dados de segurança. Use uma trilha organizacional e implantações locais de serviços de segurança de contas (Amazon GuardDuty,,, AWS Security Hub CSPM Amazon AWS Config EventBridge, IAM Access Analyzer),

que são configurados e monitorados pela equipe de segurança. Por fim, você permite que sua empresa defina os controles de forma centralizada. Você alinha a conta do aplicativo à estrutura de segurança mais ampla, tornando-a membro da OU de cargas de trabalho, por meio da qual ela herda as permissões, restrições e proteções de serviço apropriadas.

> **Considerações sobre design**
>
> Em sua organização, é provável que você tenha mais de um aplicativo de negócios. A OU de cargas de trabalho foi projetada para abrigar a maioria das cargas de trabalho específicas de sua empresa, incluindo ambientes de produção e não produção. Essas cargas de trabalho podem ser uma combinação de aplicativos comerciais off-the-shelf (COTS) e seus próprios aplicativos e serviços de dados personalizados desenvolvidos internamente. Existem poucos padrões para organizar diferentes aplicativos de negócios junto com seus ambientes de desenvolvimento. Um padrão é ter vários filhos OUs com base em seu ambiente de desenvolvimento, como produção, preparação, teste e desenvolvimento, e usar filhos Contas da AWS separados daqueles OUs que pertencem a aplicativos diferentes. Outro padrão comum é ter filhos separados OUs por aplicativo e, em seguida, usar filhos separados Contas da AWS para ambientes de desenvolvimento individuais. A estrutura exata da OU e da conta depende do design do aplicativo e das equipes que gerenciam esses aplicativos. Considere os controles de segurança que você deseja aplicar, sejam eles específicos do ambiente ou do aplicativo, porque é mais fácil implementar esses controles da mesma forma. SCPs OUs Para mais considerações sobre a organização orientada à carga de trabalho OUs, consulte a OUs seção Aplicativos do AWS whitepaper Organizando seu ambiente usando várias contas. AWS

Aplicação VPC

A nuvem privada virtual (VPC) na conta do aplicativo precisa tanto de acesso de entrada (para os serviços web simples que você está modelando) quanto de acesso de saída (para necessidades ou necessidades do aplicativo). AWS service (Serviço da AWS) Por padrão, os recursos dentro de uma VPC são roteáveis entre si. Há duas sub-redes privadas: uma para hospedar as EC2 instâncias (camada de aplicativo) e outra para o Amazon Aurora (camada de banco de dados). A segmentação da rede entre diferentes camadas, como a camada do aplicativo e a camada do banco de dados, é realizada por meio de grupos de segurança da VPC, que restringem o tráfego no nível da instância. Para maior resiliência, a carga de trabalho abrange duas ou mais zonas de disponibilidade e utiliza duas sub-redes por zona.

Considerações sobre design

Você pode usar o espelhamento de tráfego para copiar o tráfego de rede de uma interface de rede elástica de EC2 instâncias. Em seguida, você pode enviar o tráfego para dispositivos out-of-band de segurança e monitoramento para inspeção de conteúdo, monitoramento de ameaças ou solução de problemas. Por exemplo, talvez você queira monitorar o tráfego que está saindo da sua VPC ou o tráfego cuja origem está fora da sua VPC. Nesse caso, você espelhará todo o tráfego, exceto o tráfego que passa pela sua VPC, e o enviará para um único dispositivo de monitoramento. Os logs de fluxo do Amazon VPC não capturam tráfego espelhado; eles geralmente capturam informações somente dos cabeçalhos dos pacotes. O espelhamento de tráfego fornece uma visão mais profunda do tráfego da rede, permitindo que você analise o conteúdo real do tráfego, incluindo a carga útil. Ative o espelhamento de tráfego somente para a interface de rede elástica de EC2 instâncias que podem estar operando como parte de cargas de trabalho confidenciais ou para as quais você espera precisar de diagnósticos detalhados no caso de um problema.

Endpoints da VPC

Os endpoints de VPC fornecem outra camada de controle de segurança, além de escalabilidade e confiabilidade. Use-os para conectar seu aplicativo VPC a outro. Serviços da AWS(Na conta do aplicativo, o AWS SRA emprega endpoints VPC para, AWS KMS e AWS Systems Manager Amazon S3.) Endpoints são dispositivos virtuais. Eles são componentes de VPC escalados horizontalmente, redundantes e altamente disponíveis. Permitem a comunicação entre instâncias em sua VPC e serviços, sem impor riscos de disponibilidade ou restrições de largura de banda ao tráfego de rede. Você pode usar um endpoint de VPC para conectar de forma privada sua VPC a serviços de endpoint de VPC compatíveis Serviços da AWS e alimentados AWS PrivateLink por, sem precisar de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias em sua VPC não exigem endereços IP públicos para se comunicarem com outras. Serviços da AWS O tráfego entre sua VPC e a outra AWS service (Serviço da AWS) não sai da rede Amazon.

Outro benefício do uso de VPC endpoints é permitir a configuração de políticas de endpoint. Uma política de endpoint da VPC é uma política de recursos do IAM que você anexa a um endpoint quando cria ou modifica o endpoint. Se você não anexar uma política do IAM ao criar um endpoint, AWS anexe uma política do IAM padrão para você que permite acesso total ao serviço. Uma política de endpoint não substitui políticas de usuário do IAM ou políticas específicas de serviço (como

políticas de bucket do S3). É uma política do IAM separada para controlar o acesso do endpoint ao serviço especificado. Dessa forma, ele adiciona outra camada de controle sobre quais AWS diretores podem se comunicar com recursos ou serviços.

Amazon EC2

As EC2 instâncias da Amazon que compõem nosso aplicativo usam a versão 2 do Instance Metadata Service ()IMDSv2. IMDSv2 adiciona proteções para quatro tipos de vulnerabilidades que podem ser usadas para tentar acessar o IMDS: firewalls de aplicativos de sites, proxies reversos abertos, vulnerabilidades de falsificação de solicitações do lado do servidor (SSRF), firewalls abertos de camada 3 e. NATs Para obter mais informações, consulte a postagem do blog Adicione uma defesa aprofundada contra firewalls abertos, proxies reversos e vulnerabilidades de SSRF com aprimoramentos no Instance Metadata Service. EC2

Use separado VPCs (como subconjunto dos limites da conta) para isolar a infraestrutura por segmentos de carga de trabalho. Use sub-redes para isolar as camadas de sua aplicação (por exemplo, Web, aplicação e banco de dados) em uma única VPC. Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet. Para chamar a EC2 API da Amazon de sua sub-rede privada sem usar um gateway de internet, use AWS PrivateLink. Restrinja o acesso às suas instâncias usando grupos de segurança. Use os registros de fluxo da VPC para monitorar o tráfego que chega às suas instâncias. Use o Gerenciador de Sessões, um recurso do AWS Systems Manager, para acessar suas instâncias remotamente em vez de abrir portas SSH de entrada e gerenciar chaves SSH. Use volumes separados do Amazon Elastic Block Store (Amazon EBS) para o sistema operacional e seus dados. Você pode configurá-lo Conta da AWS para impor a criptografia dos novos volumes do EBS e das cópias de snapshot que você criar.

> **Exemplo de implementação**
>
> A biblioteca de códigos AWS SRA fornece um exemplo de implementação da criptografia padrão do Amazon EBS na Amazon. EC2 Ele demonstra como você pode ativar a criptografia padrão do Amazon EBS em nível de conta dentro de cada conta Conta da AWS e Região da AWS dentro da organização. AWS

AWS Enclaves Nitro

AWS O Nitro Enclaves é um EC2 recurso da Amazon que permite criar ambientes de execução isolados, chamados enclaves, a partir de instâncias. EC2 Os enclaves são máquinas virtuais

separadas, reforçadas e altamente restritas. A CPU e a memória de uma única EC2 instância principal são particionadas em enclaves isolados. Cada enclave executa um kernel independente. Os enclaves fornecem somente conectividade segura de soquetes locais com sua instância principal. Eles não têm armazenamento persistente, acesso interativo ou rede externa. Os usuários não podem usar SSH em um enclave, e os dados e aplicativos dentro do enclave não podem ser acessados pelos processos, aplicativos ou usuários (raiz ou administrador) da instância principal. Você pode proteger seus dados mais confidenciais, como informações de identificação pessoal (PII), dados de saúde, financeiros e de propriedade intelectual, dentro de instâncias. EC2 O Nitro Enclaves permite que você se concentre em seu aplicativo em vez de se preocupar com a integração com serviços externos. O Nitro Enclaves inclui atestado criptográfico para seu software, para que você tenha certeza de que somente o código autorizado está em execução e integração com o, AWS KMS para que somente seus enclaves possam acessar material confidencial. Isso ajuda a reduzir a área de superfície de ataque de seus aplicativos de processamento de dados mais confidenciais. Não há custo adicional de usar o Nitro Enclaves.

O atestado criptográfico é um processo usado para provar a identidade de um enclave. O processo de atestação é realizado por meio do Nitro Hypervisor, que produz um documento de atestação assinado para o enclave para provar sua identidade a outro terceiro ou serviço. Os documentos de atestado contêm detalhes importantes do enclave, como a chave pública do enclave, hashes da imagem e dos aplicativos do enclave e muito mais.

Com o AWS Certificate Manager (ACM) para Nitro Enclaves, você pode usar certificados públicos e privados. SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLS O ACM for Nitro Enclaves cria chaves privadas seguras, distribui o certificado e sua chave privada para seu enclave e gerencia as renovações de certificados. Com o ACM for Nitro Enclaves, a chave privada do certificado permanece isolada no enclave, o que impede que a instância e seus usuários a acessem. Para obter mais informações, consulte AWS Certificate Manager Nitro Enclaves na documentação do Nitro Enclaves.

Application Load Balancers

Os Application Load Balancers distribuem o tráfego de entrada do aplicativo em vários destinos, como EC2 instâncias, em várias zonas de disponibilidade. No AWS SRA, o grupo-alvo do balanceador de carga são as instâncias do aplicativo EC2 . O AWS SRA usa ouvintes HTTPS para garantir que o canal de comunicação seja criptografado. O Application Load Balancer usa um

certificado de servidor para encerrar a conexão front-end e depois descriptografar as solicitações dos clientes antes de enviá-las aos destinos.

AWS Certificate Manager O (ACM) se integra nativamente aos Application Load Balancers, e o AWS SRA usa o ACM para gerar e gerenciar os certificados públicos X.509 (servidor TLS) necessários. Você pode aplicar o TLS 1.2 e cifras fortes para conexões front-end por meio da política de segurança do Application Load Balancer. Para mais informações, consulte a documentação do Elastic Load Balancing.

Considerações sobre design

- Para cenários comuns, como aplicativos estritamente internos que exigem um certificado TLS privado no Application Load Balancer, você pode usar o ACM nessa conta para gerar um certificado privado a partir de. CA Privada da AWSNo AWS SRA, a CA privada raiz do ACM é hospedada na conta do Security Tooling e pode ser compartilhada com toda a AWS organização ou com entidades específicas Contas da AWS para emitir certificados de entidade final, conforme descrito anteriormente na seção Conta do Security Tooling.
- Para certificados públicos, você pode usar o ACM para gerar esses certificados e gerenciá-los, incluindo a rotação automática. Como alternativa, você pode gerar seus próprios certificados usando SSL/TLS ferramentas para criar uma solicitação de assinatura de certificado (CSR), fazer com que a CSR seja assinada por uma autoridade de certificação (CA) para produzir um certificado e, em seguida, importar o certificado para o ACM ou fazer upload do certificado no IAM para uso com o Application Load Balancer. Se você importar um certificado para o ACM, deverá monitorar a data de expiração do certificado e renová-lo antes que ele expire.
- Para obter camadas adicionais de defesa, você pode implantar AWS WAF políticas para proteger o Application Load Balancer. Ter políticas periféricas, políticas de aplicativos e até mesmo camadas de aplicação de políticas privadas ou internas aumenta a visibilidade das solicitações de comunicação e fornece uma aplicação unificada de políticas. Para obter mais informações, consulte a postagem do blog Implantando defesa em profundidade usando AWS Managed Rules for AWS WAF.

CA Privada da AWS

Autoridade de Certificação Privada da AWS(CA Privada da AWS) é usado na conta do aplicativo para gerar certificados privados para serem usados com um Application Load Balancer. É um cenário comum que os Application Load Balancers forneçam conteúdo seguro via TLS. Isso exige que os certificados TLS sejam instalados no Application Load Balancer. Para aplicativos estritamente internos, os certificados TLS privados podem fornecer o canal seguro.

No AWS SRA, CA Privada da AWS está hospedado na conta do Security Tooling e é compartilhado com a conta do aplicativo usando. AWS RAM Isso permite que os desenvolvedores em uma conta de aplicativo solicitem um certificado de uma CA privada compartilhada. Compartilhar CAs em toda a sua organização ou entre Contas da AWS ela ajuda a reduzir o custo e a complexidade de criar e gerenciar duplicatas CAs em todos os seus Contas da AWS. Quando você usa o ACM para emitir certificados privados de uma CA compartilhada, o certificado é gerado localmente na conta solicitante, e o ACM fornece gerenciamento e renovação completos do ciclo de vida.

Amazon Inspector

O AWS SRA usa o Amazon Inspector para descobrir e EC2 verificar automaticamente instâncias e imagens de contêineres que residem no Amazon Elastic Container Registry (Amazon ECR) em busca de vulnerabilidades de software e exposição não intencional na rede.

O Amazon Inspector é colocado na conta do aplicativo porque fornece serviços de gerenciamento de vulnerabilidades para EC2 instâncias dessa conta. Além disso, o Amazon Inspector relata caminhos de rede indesejados de e para instâncias EC2 .

O Amazon Inspector nas contas dos membros é gerenciado centralmente pela conta do administrador delegado. No AWS SRA, a conta do Security Tooling é a conta do administrador delegado. A conta de administrador delegado pode gerenciar descobertas, dados e determinadas configurações para membros da organização. Isso inclui a visualização de detalhes agregados das descobertas de todas as contas dos membros, a ativação ou desativação das verificações das contas dos membros e a revisão dos recursos escaneados dentro da organização. AWS

> **Considerações sobre design**
>
> Você pode usar o Patch Manager, um recurso do AWS Systems Manager, para acionar patches sob demanda para remediar vulnerabilidades de dia zero ou outras vulnerabilidades críticas de segurança do Amazon Inspector. O Patch Manager ajuda você a corrigir essas

vulnerabilidades sem ter que esperar pelo cronograma normal de patches. A remediação é realizada usando o runbook do Systems Manager Automation. Para obter mais informações, consulte a série de blogs em duas partes Automatize o gerenciamento e a remediação de vulnerabilidades usando o Amazon AWS Inspector e. AWS Systems Manager

AWS Systems Manager

AWS Systems Manageré um AWS service (Serviço da AWS) que você pode usar para visualizar dados operacionais de várias tarefas Serviços da AWS e automatizar tarefas operacionais em seus AWS recursos. Com fluxos de trabalho e runbooks de aprovação automatizados, você pode trabalhar para reduzir o erro humano e simplificar as tarefas de manutenção e implantação dos recursos. AWS

Além desses recursos gerais de automação, o Systems Manager oferece suporte a vários recursos de segurança preventivos, de detecção e responsivos. AWS Systems Manager Agent (SSM Agent) é um software da Amazon que pode ser instalado e configurado em uma EC2 instância, em um servidor local ou em uma máquina virtual (VM). O SSM Agent permite que o Systems Manager atualize, gerencie e configure esses recursos. O Systems Manager ajuda você a manter a segurança e a conformidade examinando essas instâncias gerenciadas e relatando (ou tomando medidas corretivas) sobre quaisquer violações detectadas em seu patch, configuração e políticas personalizadas.

O AWS SRA usa o Session Manager, um recurso do Systems Manager, para fornecer uma experiência interativa de shell e CLI baseada em navegador. Isso fornece gerenciamento de instâncias seguro e auditável sem a necessidade de abrir portas de entrada, manter bastion hosts ou gerenciar chaves SSH. O AWS SRA usa o Patch Manager, um recurso do Systems Manager, para aplicar patches às EC2 instâncias de sistemas operacionais e aplicativos.

O AWS SRA também usa a automação, um recurso do Systems Manager, para simplificar as tarefas comuns de manutenção e implantação de EC2 instâncias e outros AWS recursos da Amazon. A automação pode simplificar tarefas comuns de TI como alterar o estado de um ou mais nós gerenciados (usando uma automação de aprovação) e gerenciar estados dos nós gerenciados de acordo com sua própria programação. O Systems Manager inclui recursos que ajudam você a direcionar grandes grupos de instâncias usando etiquetas e controles de velocidade que ajudam a implementar alterações de acordo com os limites que você define. A automação oferece automações com um clique para simplificar tarefas complexas, como criar imagens douradas da Amazon Machine (AMIs) e recuperar instâncias inacessíveis. EC2 Além disso, você pode aprimorar a segurança

operacional dando às funções do IAM acesso a runbooks específicos para realizar determinadas funções, sem conceder permissões diretamente a essas funções. Por exemplo, se você quiser que uma função do IAM tenha permissões para reiniciar EC2 instâncias específicas após atualizações de patches, mas não quiser conceder a permissão diretamente a essa função, crie um runbook de automação e conceda à função permissões para executar somente o runbook.

Considerações sobre design

- O Systems Manager depende dos metadados da EC2 instância para funcionar corretamente. O Systems Manager pode acessar os metadados da instância usando a versão 1 ou a versão 2 do Instance Metadata Service (IMDSv1 e IMDSv2).
- O SSM Agent precisa se comunicar com diferentes Serviços da AWS recursos, como EC2 mensagens da Amazon, Systems Manager e Amazon S3. Para que essa comunicação ocorra, a sub-rede exige conectividade de saída com a Internet ou provisionamento de VPC endpoints apropriados. O AWS SRA usa endpoints VPC para que o agente SSM estabeleça caminhos de rede privados para vários. Serviços da AWS
- Usando o Automation, você pode compartilhar as práticas recomendadas com o restante da sua organização. Você pode criar as melhores práticas para gerenciamento de recursos em runbooks e compartilhar os runbooks entre grupos Regiões da AWS . Você também pode restringir os valores permitidos para os parâmetros do runbook. Para esses casos de uso, talvez seja necessário criar runbooks de automação em uma conta central, como ferramentas de segurança ou serviços compartilhados, e compartilhá-los com o resto da AWS organização. Os casos de uso comuns incluem a capacidade de implementar centralmente atualizações de patches e segurança, corrigir desvios nas configurações de VPC ou nas políticas de bucket do S3 e gerenciar instâncias em grande escala. EC2 Para obter detalhes sobre a implementação, consulte a documentação do Systems Manager.

Amazon Aurora

No AWS SRA, o Amazon Aurora e o Amazon S3 compõem a camada lógica de dados. O Aurora é um mecanismo de banco de dados relacional gerenciado compatível com o MySQL e o PostgreSQL. Um aplicativo que está sendo executado nas EC2 instâncias se comunica com o Aurora e o Amazon S3 conforme necessário. O Aurora é configurado com um cluster de banco de dados dentro de um grupo de sub-redes de banco de dados.

Considerações sobre design

Como em muitos serviços de banco de dados, a segurança do Aurora é gerenciada em três níveis. Para controlar quem pode realizar ações de gerenciamento do Amazon Relational Database Service (Amazon RDS) em clusters e instâncias de banco de dados Aurora, você usa o IAM. Para controlar quais dispositivos e EC2 instâncias podem abrir conexões com o endpoint do cluster e a porta da instância de banco de dados para clusters de banco de dados Aurora em uma VPC, você usa um grupo de segurança da VPC. Para autenticar logins e permissões para um cluster de banco de dados Aurora, você pode adotar a mesma abordagem de uma instância de banco de dados independente do MySQL ou do PostgreSQL, ou pode usar a autenticação do banco de dados do IAM para a edição compatível com o Aurora MySQL. Com essa última abordagem, você se autentica em seu cluster de banco de dados compatível com o Aurora MySQL usando uma função do IAM e um token de autenticação.

Amazon S3

O Amazon S3 é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e performance líderes do setor. É a espinha dorsal de dados de muitos aplicativos desenvolvidos AWS, e as permissões e os controles de segurança apropriados são essenciais para proteger dados confidenciais. Para obter as melhores práticas de segurança recomendadas para o Amazon S3, consulte a documentação, palestras técnicas on-line e análises mais detalhadas nas postagens do blog. A melhor prática mais importante é bloquear o acesso excessivamente permissivo (especialmente o acesso público) aos buckets do S3.

AWS KMS

O AWS SRA ilustra o modelo de distribuição recomendado para o gerenciamento de chaves, em que elas AWS KMS key residem dentro do Conta da AWS mesmo recurso a ser criptografado. Por esse motivo, AWS KMS é usado na conta do aplicativo, além de ser incluído na conta do Security Tooling. Na conta do aplicativo, AWS KMS é usado para gerenciar chaves específicas dos recursos do aplicativo. Você pode implementar uma separação de tarefas usando políticas de chaves para conceder permissões de uso de chaves às funções locais do aplicativo e restringir as permissões de gerenciamento e monitoramento aos seus principais guardiões.

Considerações sobre design

Em um modelo distribuído, a AWS KMS principal responsabilidade do gerenciamento é da equipe de aplicativos. No entanto, sua equipe central de segurança pode ser responsável pela governança e pelo monitoramento de eventos criptográficos importantes, como os seguintes:

- O material da chave importada em uma chave do KMS está próximo da data de validade.
- O material de chave em uma chave do KMS foi alternado automaticamente.
- A chave AKMS foi excluída.
- Há uma alta taxa de falha na decodificação.

AWS CloudHSM

AWS CloudHSMfornece módulos gerenciados de segurança de hardware (HSMs) no Nuvem AWS. Ele permite que você gere e use suas próprias chaves de criptografia AWS usando o FIPS 140-2 nível 3 validado, ao HSMs qual você controla o acesso. Você pode usar AWS CloudHSM para descarregar o SSL/TLS processamento de seus servidores web. Isso reduz a carga sobre o servidor da Web e fornece segurança extra ao armazenar a chave privada do servidor da Web AWS CloudHSM. Da mesma forma, você pode implantar um HSM a partir da AWS CloudHSM VPC de entrada na conta de rede para armazenar suas chaves privadas e assinar solicitações de certificado se precisar atuar como autoridade de certificação emissora.

Considerações sobre design

Se você tiver um requisito rígido para o FIPS 140-2 nível 3, também poderá optar por configurar AWS KMS o uso do AWS CloudHSM cluster como um armazenamento de chaves personalizado em vez de usar o armazenamento de chaves KMS nativo. Ao fazer isso, você se beneficia da integração entre AWS KMS e Serviços da AWS que criptografa seus dados, ao mesmo tempo em HSMs que é responsável pela proteção de suas chaves KMS. Isso combina um único inquilino HSMs sob seu controle com a facilidade de uso e integração do. AWS KMS Para gerenciar sua AWS CloudHSM infraestrutura, você precisa empregar uma infraestrutura de chave pública (PKI) e ter uma equipe com experiência em gerenciamento. HSMs

AWS Secrets Manager

AWS Secrets Managerajuda a proteger as credenciais (segredos) de que você precisa para acessar seus aplicativos, serviços e recursos de TI. O serviço permite que você alterne, gerencie e recupere com eficiência as credenciais do banco de dados, as chaves de API e outros segredos durante todo o ciclo de vida. Você pode substituir as credenciais codificadas em seu código por uma chamada de API para o Secrets Manager para recuperar o segredo programaticamente. Isso ajuda a garantir que o segredo não possa ser comprometido por alguém que esteja examinando seu código, porque o segredo não existe mais no código. Além disso, o Secrets Manager ajuda você a mover seus aplicativos entre ambientes (desenvolvimento, pré-produção, produção). Em vez de alterar o código, você pode garantir que um segredo devidamente nomeado e referenciado esteja disponível no ambiente. Isso promove a consistência e a reutilização do código do aplicativo em diferentes ambientes, ao mesmo tempo em que exige menos alterações e interações humanas após o teste do código.

Com o Secrets Manager, você pode gerenciar o acesso aos segredos usando políticas de IAM refinadas e políticas baseadas em recursos. Você pode ajudar a proteger segredos criptografando-os com chaves de criptografia que você gerencia usando AWS KMS. O Secrets Manager também se integra aos serviços de AWS registro e monitoramento para auditoria centralizada.

O Secrets Manager usa criptografia de envelope AWS KMS keys e chaves de dados para proteger cada valor secreto. Ao criar um segredo, você pode escolher qualquer chave simétrica gerenciada pelo cliente na região Conta da AWS e ou pode usar a chave AWS gerenciada para o Secrets Manager.

Como prática recomendada, você pode monitorar seus segredos para registrar quaisquer alterações neles. Isso ajuda a garantir que qualquer uso ou alteração inesperada possa ser investigada. Alterações indesejadas podem ser revertidas. Atualmente, o Secrets Manager oferece suporte a dois Serviços da AWS que permitem monitorar sua organização e atividade: AWS CloudTrail AWS Config e. CloudTrail captura todas as chamadas de API para o Secrets Manager como eventos, incluindo chamadas do console do Secrets Manager e de chamadas de código para o Secrets Manager APIs. Além disso, CloudTrail captura outros eventos relacionados (não relacionados à API) que podem ter um impacto na segurança ou na conformidade Conta da AWS ou podem ajudá-lo a solucionar problemas operacionais. Isso inclui certos eventos de rotação de segredos e exclusão de versões secretas. AWS Config pode fornecer controles de detetive rastreando e monitorando alterações nos segredos no Secrets Manager. Essas alterações incluem a descrição de um segredo, a configuração de rotação, as tags e o relacionamento com outras AWS fontes, como a chave de criptografia KMS ou as AWS Lambda funções usadas para rotação secreta. Você também pode configurar a Amazon

EventBridge, que recebe notificações de alteração de configuração e conformidade AWS Config, para rotear eventos secretos específicos para ações de notificação ou remediação.

No AWS SRA, o Secrets Manager está localizado na conta do aplicativo para oferecer suporte a casos de uso de aplicativos locais e gerenciar segredos próximos ao seu uso. Aqui, um perfil de instância é anexado às EC2 instâncias na conta do aplicativo. Segredos separados podem então ser configurados no Secrets Manager para permitir que esse perfil de instância recupere segredos — por exemplo, para ingressar no domínio apropriado do Active Directory ou LDAP e acessar o banco de dados Aurora. O Secrets Manager se integra ao Amazon RDS para gerenciar as credenciais do usuário quando você cria, modifica ou restaura uma instância de banco de dados Amazon RDS ou um cluster de banco de dados Multi-AZ. Isso ajuda você a gerenciar a criação e a rotação de chaves e substitui as credenciais codificadas em seu código por chamadas programáticas de API para o Secrets Manager.

> **Considerações sobre design**
>
> Em geral, configure e gerencie o Secrets Manager na conta mais próxima de onde os segredos serão usados. Essa abordagem aproveita o conhecimento local do caso de uso e fornece velocidade e flexibilidade às equipes de desenvolvimento de aplicativos. Para informações rigorosamente controladas, nas quais uma camada adicional de controle pode ser apropriada, os segredos podem ser gerenciados centralmente pelo Secrets Manager na conta do Security Tooling.

Amazon Cognito

O Amazon Cognito permite que você adicione cadastro, login e controle de acesso de usuários aos seus aplicativos web e móveis de forma rápida e eficiente. O Amazon Cognito é escalável para milhões de usuários e oferece suporte ao login com provedores de identidade social, como Apple, Facebook, Google e Amazon, e provedores de identidade corporativa por meio do SAML 2.0 e do OpenID Connect. Os dois principais componentes do Amazon Cognito são grupos de usuários e grupos de identidades. Os grupos de usuários são diretórios de usuários que fornecem opções de inscrição e login para os usuários do seu aplicativo. Os grupos de identidades permitem que você conceda aos seus usuários acesso a outros Serviços da AWS. Você pode usar grupos de identidades e grupos de usuários separadamente ou em conjunto. Para cenários de uso comuns, consulte a documentação do Amazon Cognito.

O Amazon Cognito fornece uma interface de usuário integrada e personalizável para cadastro e login de usuários. Você pode usar o Android, o iOS e JavaScript SDKs o Amazon Cognito para adicionar páginas de cadastro e login de usuários aos seus aplicativos. O Amazon Cognito Sync é uma AWS service (Serviço da AWS) biblioteca cliente que permite a sincronização entre dispositivos de dados de usuários relacionados ao aplicativo.

O Amazon Cognito oferece suporte à autenticação multifatorial e à criptografia de dados em repouso e dados em trânsito. Os grupos de usuários do Amazon Cognito fornecem recursos de segurança avançados para ajudar a proteger o acesso às contas de usuário em seu aplicativo. Esses recursos avançados de segurança fornecem autenticação adaptativa baseada em risco e proteção contra o uso de credenciais comprometidas.

Considerações sobre design

- Você pode criar uma AWS Lambda função e, em seguida, acionar essa função durante as operações do grupo de usuários, como inscrição, confirmação e login (autenticação) do usuário com um gatilho Lambda. Você pode adicionar desafios de autenticação, migrar usuários e personalizar mensagens de verificação. Para operações comuns e fluxo de usuários, consulte a documentação do Amazon Cognito. O Amazon Cognito chama as funções do Lambda de forma síncrona.
- Você pode usar grupos de usuários do Amazon Cognito para proteger aplicativos pequenos e multilocatários. Um caso de uso comum do design multilocatário é executar cargas de trabalho para dar suporte ao teste de várias versões de um aplicativo. O projeto de vários locatários também é útil para testar uma única aplicação com diferentes conjuntos de dados, o que permite o uso completo dos seus recursos de cluster. No entanto, certifique-se de que o número de inquilinos e o volume esperado estejam alinhados com as cotas de serviço relacionadas do Amazon Cognito. Essas cotas são compartilhadas entre todos os locatários da aplicação.

Amazon Verified Permissions

O Amazon Verified Permissions é um serviço de gerenciamento de permissões escalável e de autorização refinado para os aplicativos que você cria. Desenvolvedores e administradores podem usar o Cedar, uma linguagem de políticas de código aberto criada especificamente e que prioriza a segurança, com funções e atributos para definir controles de acesso mais granulares, contextuais e baseados em políticas. Os desenvolvedores podem criar aplicativos mais seguros com mais rapidez

externalizando a autorização e centralizando o gerenciamento e a administração de políticas. As permissões verificadas incluem definições de esquema, gramática de declarações de política e raciocínio automatizado que abrangem milhões de permissões, para que você possa aplicar os princípios de negação padrão e privilégio mínimo. O serviço também inclui uma ferramenta de simulador de avaliação para ajudá-lo a testar suas decisões de autorização e políticas de autores. Esses recursos facilitam a implantação de um modelo de autorização detalhado e refinado para apoiar seus objetivos de confiança zero. As Permissões Verificadas centralizam as permissões em um repositório de políticas e ajudam os desenvolvedores a usar essas permissões para autorizar ações do usuário em seus aplicativos.

Você pode conectar seu aplicativo ao serviço por meio da API para autorizar as solicitações de acesso do usuário. Para cada solicitação de autorização, o serviço recupera as políticas relevantes e avalia essas políticas para determinar se um usuário tem permissão para realizar uma ação em um recurso, com base nas entradas de contexto, como usuários, funções, associação ao grupo e atributos. Você pode configurar e conectar Permissões Verificadas para enviar seus registros de autorização e gerenciamento de políticas para AWS CloudTrail o. Se você usa o Amazon Cognito como seu repositório de identidade, você pode se integrar às Permissões Verificadas e usar o ID e os tokens de acesso que o Amazon Cognito retorna nas decisões de autorização em seus aplicativos. Você fornece tokens do Amazon Cognito para Permissões Verificadas, que usam os atributos que os tokens contêm para representar o principal e identificar os direitos do principal. Para obter mais informações sobre essa integração, consulte a postagem do AWS blog Simplificando a autorização refinada com as Permissões Verificadas da Amazon e o Amazon Cognito.

As permissões verificadas ajudam você a definir o controle de acesso baseado em políticas (PBAC). O PBAC é um modelo de controle de acesso que usa permissões expressas como políticas para determinar quem pode acessar quais recursos em um aplicativo. O PBAC reúne controle de acesso baseado em função (RBAC) e controle de acesso baseado em atributos (ABAC), resultando em um modelo de controle de acesso mais poderoso e flexível. Para saber mais sobre o PBAC e como você pode criar um modelo de autorização usando permissões verificadas, consulte a postagem do AWS blog Controle de acesso baseado em políticas no desenvolvimento de aplicativos com Amazon Verified Permissions.

No AWS SRA, as permissões verificadas estão localizadas na conta do aplicativo para oferecer suporte ao gerenciamento de permissões para aplicativos por meio de sua integração com o Amazon Cognito.

Defesa em camadas

A conta do aplicativo oferece uma oportunidade de ilustrar princípios de defesa em camadas que permitem. AWS Considere a segurança das EC2 instâncias que compõem o núcleo de um aplicativo de exemplo simples representado na AWS SRA e você poderá ver como Serviços da AWS funcionam juntas em uma defesa em camadas. Essa abordagem se alinha à visão estrutural dos serviços de AWS segurança, conforme descrito na seção Aplicar serviços de segurança em sua AWS organização, anteriormente neste guia.

- A camada mais interna são as instâncias. EC2 Conforme mencionado anteriormente, EC2 as instâncias incluem muitos recursos de segurança nativos, por padrão ou como opções. Os exemplos incluem IMDSv2o sistema Nitro e a criptografia de armazenamento Amazon EBS.
- A segunda camada de proteção se concentra no sistema operacional e no software em execução nas EC2 instâncias. Serviços como o Amazon Inspector AWS Systems Managerpermitem que você monitore, relate e tome medidas corretivas nessas configurações. O Amazon Inspector monitora seu software em busca de vulnerabilidades e o Systems Manager ajuda você a trabalhar para manter a segurança e a conformidade examinando as instâncias gerenciadas quanto ao status de patch e configuração e, em seguida, relatando e tomando as ações corretivas que você especificar.
- As instâncias e o software executado nessas instâncias dependem da sua infraestrutura AWS de rede. Além de usar os recursos de segurança da Amazon VPC, a AWS SRA também usa endpoints de VPC para fornecer conectividade privada entre a VPC e a VPC suportada Serviços da AWS, além de fornecer um mecanismo para colocar políticas de acesso no limite da rede.
- A atividade e a configuração das EC2 instâncias, do software, da rede e das funções e recursos do IAM são monitoradas ainda mais por serviços Conta da AWS focados AWS Security Hub CSPM, como, Amazon AWS Security Hub, GuardDuty, AWS CloudTrail AWS Config, IAM Access Analyzer e Amazon Macie.
- Por fim, além da conta do aplicativo, AWS RAM ajuda a controlar quais recursos são compartilhados com outras contas, e as políticas de controle de serviços do IAM ajudam a aplicar permissões consistentes em toda a AWS organização.

AI/ML para segurança

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Inteligência artificial e aprendizado de máquina (AI/ML) is transforming businesses. AI/MLtem sido o foco da Amazon há mais de 20 anos), e muitos dos recursos que os clientes usam AWS, incluindo serviços de segurança, são orientados pela IA/ML. Isso cria um valor diferenciado incorporado, pois você pode desenvolver com segurança AWS sem exigir que suas equipes de segurança ou desenvolvimento de aplicativos tenham experiência em IA/ML.

A IA é uma tecnologia avançada que permite que máquinas e sistemas obtenham inteligência e capacidade de previsão. Os sistemas de IA aprendem com experiências passadas por meio de dados que consomem ou nos quais são treinados. O ML é um dos aspectos mais importantes da IA. ML é a capacidade dos computadores de aprender com os dados sem serem programados explicitamente. Na programação tradicional, o programador escreve regras que definem como o programa deve funcionar em um computador ou máquina. No ML, o modelo aprende as regras a partir dos dados. Os modelos de ML podem descobrir padrões ocultos nos dados ou fazer previsões precisas sobre novos dados que não foram usados durante o treinamento. Serviços da AWS Uso múltiplo AI/ML para aprender com grandes conjuntos de dados e fazer inferências de segurança.

- O Amazon Macie é um serviço de segurança de dados que usa ML e correspondência de padrões para descobrir e ajudar a proteger seus dados confidenciais. O Macie detecta automaticamente uma lista grande e crescente de tipos de dados confidenciais, incluindo informações de identificação pessoal (PII), como nomes, endereços e informações financeiras, como números de cartão de crédito. Também oferece visibilidade constante dos dados armazenados no Amazon Simple Storage Service (Amazon S3). O Macie usa modelos de processamento de linguagem natural (NLP) e ML que são treinados em diferentes tipos de conjuntos de dados para entender seus dados existentes e atribuir valores comerciais para priorizar dados essenciais aos negócios. Em seguida, Macie gera descobertas de dados confidenciais.
- GuardDutyA Amazon é um serviço de detecção de ameaças que usa ML, detecção de anomalias e inteligência de ameaças integrada para monitorar continuamente atividades maliciosas e comportamentos não autorizados para ajudar a proteger suas instâncias Contas da AWS, cargas de trabalho sem servidor e contêineres, usuários, bancos de dados e armazenamento. GuardDuty incorpora técnicas de ML que são altamente eficazes para distinguir a atividade potencialmente

maliciosa do usuário do comportamento operacional anômalo, mas benigno. Contas da AWS Esse recurso modela continuamente as invocações de API em uma conta e incorpora previsões probabilísticas para isolar e alertar com mais precisão sobre comportamentos altamente suspeitos do usuário. Essa abordagem ajuda a identificar atividades maliciosas associadas a táticas de ameaças conhecidas, incluindo descoberta, acesso inicial, persistência, escalonamento de privilégios, evasão de defesa, acesso a credenciais, impacto e exfiltração de dados. Para saber mais sobre como GuardDuty usa o aprendizado de máquina, consulte a sessão de AWS discussão do re:Inforce 2023 Desenvolvendo novas descobertas usando o aprendizado de máquina na Amazon GuardDuty (0). TDR31

Segurança comprovada

AWS desenvolve ferramentas de raciocínio automatizadas que usam lógica matemática para responder perguntas críticas sobre sua infraestrutura e detectar configurações incorretas que poderiam potencialmente expor seus dados. Esse recurso é chamado de segurança comprovada porque fornece maior garantia na segurança da nuvem e na nuvem. A segurança comprovada usa o raciocínio automatizado, que é uma disciplina específica da IA que aplica a dedução lógica aos sistemas de computador. Por exemplo, ferramentas de raciocínio automatizado podem analisar políticas e configurações de arquitetura de rede e provar a ausência de configurações não intencionais que poderiam potencialmente expor dados vulneráveis. Essa abordagem fornece o mais alto nível de garantia possível para as características críticas de segurança da nuvem. Para obter mais informações, consulte Recursos de segurança comprovados no AWS site. Atualmente, Serviços da AWS os recursos a seguir usam raciocínio automatizado para ajudar você a obter segurança comprovada para seus aplicativos:

- O Amazon Verified Permissions é um serviço de gerenciamento de permissões escalável e de autorização refinado para os aplicativos que você cria. O Verified Permissions usa o Cedar, que é uma linguagem de código aberto para controle de acesso que foi criada usando raciocínio automatizado e testes diferenciais. O Cedar é uma linguagem para definir permissões como políticas que descrevem quem deve ter acesso a quais recursos. É também uma especificação para avaliar essas políticas. Use as políticas do Cedar para controlar o que cada usuário do seu aplicativo tem permissão para fazer e quais recursos eles podem acessar. As políticas do Cedar são declarações de permissão ou proibição que determinam se um usuário pode agir em um recurso. As políticas estão associadas aos recursos e você pode anexar várias políticas a um recurso. As políticas de proibição substituem as políticas de permissão. Quando um usuário do seu aplicativo tenta realizar uma ação em um recurso, seu aplicativo faz uma solicitação

de autorização ao mecanismo de políticas do Cedar. A Cedar avalia as políticas aplicáveis e retorna uma decisão `ALLOW` ou`DENY`. O Cedar suporta regras de autorização para qualquer tipo de principal e recurso, permite o controle de acesso baseado em funções e atributos e oferece suporte à análise por meio de ferramentas de raciocínio automatizadas que podem ajudar a otimizar suas políticas e validar seu modelo de segurança.

- AWS Identity and Access Management Access Analyzerajuda você a simplificar o gerenciamento de permissões. Você pode usar esse recurso para definir permissões refinadas, verificar as permissões pretendidas e refinar as permissões removendo o acesso não utilizado. O IAM Access Analyzer gera uma política refinada com base na atividade de acesso capturada em seus registros. Ele também fornece mais de 100 verificações de políticas para ajudá-lo a criar e validar suas políticas. O IAM Access Analyzer usa segurança comprovada para analisar caminhos de acesso e fornecer descobertas abrangentes para acesso público e entre contas aos seus recursos. Essa ferramenta é baseada em Zelkova, que traduz as políticas do IAM em declarações lógicas equivalentes e executa um conjunto de solucionadores lógicos especializados e de uso geral (teorias do módulo de satisfatabilidade) contra o problema. O IAM Access Analyzer aplica o Zelkova repetidamente a uma política com consultas cada vez mais específicas para caracterizar classes de comportamentos que a política permite, com base no conteúdo da política. O analisador não examina os registros de acesso para determinar se uma entidade externa acessou um recurso dentro da sua zona de confiança. Ela gera uma descoberta quando uma política baseada em recursos permite o acesso a um recurso, mesmo que o recurso não tenha sido acessado pela entidade externa. Para saber mais sobre as teorias do módulo de satisfatabilidade, consulte Teorias do módulo de satisfatabilidade no Handbook of Satisfiability. *
- O Amazon S3 Block Public Access é um recurso do Amazon S3 que permite bloquear possíveis configurações incorretas que possam levar ao acesso público de seus buckets e objetos. Você pode habilitar o Amazon S3 Block Public Access para pontos de acesso, buckets, contas e para a AWS organização (o que afeta os buckets existentes e novos na conta). O acesso público é concedido a buckets e objetos por meio de listas de controle de acesso (ACLs), políticas de bucket ou ambas. A determinação de se uma determinada política ou ACL é considerada pública é feita usando o sistema de raciocínio automatizado Zelkova. O Amazon S3 usa o Zelkova para verificar cada política de bucket e avisa se um usuário não autorizado conseguir ler ou gravar em seu bucket. Se um bucket for marcado como público, algumas solicitações públicas poderão acessar o bucket. Se um bucket for marcado como não público, todas as solicitações públicas serão negadas. Zelkova é capaz de fazer essas determinações porque tem uma representação matemática precisa das políticas do IAM. Ele cria uma fórmula para cada política e prova um teorema sobre essa fórmula.

- O Amazon VPC Network Access Analyzer é um recurso do Amazon VPC que ajuda você a entender possíveis caminhos de rede para seus recursos e a identificar possíveis acessos não intencionais à rede. O Network Access Analyzer ajuda você a verificar a segmentação da rede, identificar a acessibilidade da Internet e verificar caminhos de rede confiáveis e acesso à rede. Esse recurso usa algoritmos de raciocínio automatizado para analisar os caminhos de rede que um pacote pode percorrer entre os recursos em uma AWS rede. Em seguida, ele produz descobertas para caminhos que correspondem aos seus escopos de acesso à rede, que definem padrões de tráfego de saída e entrada. O Analisador de Acesso à Rede executa uma análise estática de uma configuração de rede, o que significa que nenhum pacote é transmitido na rede como parte dessa análise.
- O Amazon VPC Reachability Analyzer é um recurso do Amazon VPC que permite depurar, entender e visualizar a conectividade em sua rede. AWS O Reachability Analyzer é uma ferramenta de análise de configuração que permite realizar testes de conectividade entre um recurso de origem e um recurso de destino em suas nuvens privadas virtuais (). VPCs Quando o destino está acessível, o Reachability hop-by-hop Analyzer produz detalhes do caminho da rede virtual entre a origem e o destino. Quando o destino não está acessível, o Reachability Analyzer identifica o componente de bloqueio. O Reachability Analyzer usa raciocínio automatizado para identificar caminhos viáveis criando um modelo da configuração da rede entre a origem e o destino. Em seguida, ele verifica a acessibilidade com base na configuração. Ele não envia pacotes nem analisa o plano de dados.

[*] Biere, A. M. Heule, H. van Maaren e T. Walsh. 2009. Manual de Satisfabilidade. Imprensa IOS, NLD.

Construindo sua arquitetura de segurança — uma abordagem em fases

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

A arquitetura de segurança de várias contas recomendada pela AWS SRA é uma arquitetura básica para ajudá-lo a injetar segurança logo no início do processo de design. A jornada de nuvem de cada organização é única. Para desenvolver com sucesso sua arquitetura de segurança na nuvem, você precisa visualizar o estado desejado, entender sua prontidão atual para a nuvem e adotar uma abordagem ágil para preencher quaisquer lacunas. O AWS SRA fornece um estado alvo de referência para sua arquitetura de segurança. A transformação incremental permite que você demonstre valor rapidamente e, ao mesmo tempo, minimize a necessidade de fazer previsões de longo alcance.

O AWS Cloud Adoption Framework (AWS CAF) recomenda quatro fases iterativas e incrementais de transformação da nuvem: prever, alinhar, lançar e escalar. Ao entrar na fase de lançamento e se concentrar na entrega de iniciativas-piloto na produção, você deve se concentrar em criar uma arquitetura de segurança forte como base para a fase de escala, para que você tenha a capacidade técnica de migrar e operar suas cargas de trabalho mais críticas aos negócios com confiança. Essa abordagem em fases é aplicável se você for uma startup, uma pequena ou média empresa que deseja expandir seus negócios ou uma empresa que está adquirindo novas unidades de negócios ou passando por fusões e aquisições. O AWS SRA ajuda você a alcançar essa arquitetura básica de segurança para que você possa aplicar os controles de segurança uniformemente em toda a sua organização em expansão em. AWS Organizations A arquitetura básica consiste em vários Contas da AWS serviços. O planejamento e a implementação devem ser um processo de várias fases para que você possa iterar em marcos menores para alcançar a meta maior de configurar sua arquitetura de segurança básica. Esta seção descreve as fases típicas de sua jornada para a nuvem com base em uma abordagem estruturada. Essas fases se alinham aos princípios de design de segurança do AWS Well-Architected Framework.

Fase 1: Construa sua OU e estrutura de contas

Um pré-requisito para uma base de segurança sólida é uma AWS organização e uma estrutura de contas bem projetadas. Conforme explicado anteriormente na seção de componentes básicos do SRA deste guia, ter vários Contas da AWS ajuda a isolar diferentes funções comerciais e de segurança por design. Isso pode parecer um trabalho desnecessário no começo, mas é um investimento para ajudar você a escalar com rapidez e segurança. Essa seção também explica como você pode usar AWS Organizations para gerenciar várias Contas da AWS e como usar o acesso confiável e os recursos de administrador delegado para gerenciar centralmente essas Serviços da AWS várias contas.

Você pode usar AWS Control Towerconforme descrito anteriormente neste guia para orquestrar sua landing zone. Se você estiver usando uma única Conta da AWS, consulte o Contas da AWS guia Transição para várias para migrar para várias contas o mais rápido possível. Por exemplo, se sua startup está atualmente idealizando e prototipando seu produto em um único produto Conta da AWS, você deve pensar em adotar uma estratégia de várias contas antes de lançar seu produto no mercado. Da mesma forma, organizações pequenas, médias e corporativas devem começar a criar sua estratégia de várias contas assim que planejarem suas cargas de trabalho de produção iniciais. Comece com sua base OUs e Contas da AWS, em seguida, adicione suas contas e relacionadas à carga de trabalho OUs .

Para obter Conta da AWS recomendações de estrutura de OU além das fornecidas no AWS SRA, consulte a postagem no blog Estratégia de várias contas para pequenas e médias empresas. Ao finalizar sua OU e a estrutura da conta, considere os controles de segurança de alto nível em toda a organização que você gostaria de aplicar usando políticas de controle de serviços (SCPs), políticas de controle de recursos () e políticas declarativas. RCPs

Considerações sobre design

Não replique a estrutura de relatórios da sua empresa ao projetar sua OU e estrutura de contas. Você OUs deve se basear nas funções da carga de trabalho e em um conjunto comum de controles de segurança que se aplicam às cargas de trabalho. Não tente criar sua estrutura de conta completa desde o início. Concentre-se no básico e OUs, em seguida, adicione a carga de trabalho OUs conforme necessário. Você pode mover contas entre OUs elas para experimentar abordagens alternativas durante os estágios iniciais do seu design. No entanto, isso pode resultar em alguma sobrecarga no gerenciamento de permissões

lógicas SCPs RCPs, dependendo das políticas declarativas e das condições do IAM baseadas na UO e nos caminhos da conta.

Exemplo de implementação

A biblioteca de códigos AWS SRA fornece um exemplo de implementação de contatos alternativos de conta. Essa solução define os contatos alternativos de cobrança, operações e segurança para todas as contas em uma organização.

Fase 2: Implementar uma base sólida de identidade

Depois de criar várias Contas da AWS, você deve dar às suas equipes acesso aos AWS recursos dessas contas. Há duas categorias gerais de gerenciamento de identidade: gerenciamento de identidade e acesso da força de trabalho e gerenciamento de identidade e acesso do cliente (CIAM). O Workforce IAM é para organizações nas quais funcionários e cargas de trabalho automatizadas precisam fazer login AWS para realizar seus trabalhos. O CIAM é usado quando uma organização precisa de uma forma de autenticar usuários para fornecer acesso aos aplicativos da organização. Primeiro, você precisa de uma estratégia de IAM para a força de trabalho, para que suas equipes possam criar e migrar aplicativos. Você deve sempre usar funções do IAM em vez de usuários do IAM para fornecer acesso a usuários humanos ou de máquinas. Siga as orientações da AWS SRA sobre como usar as contas Centro de Identidade do AWS IAM de gerenciamento de organizações e serviços compartilhados para gerenciar centralmente o acesso de login único (SSO) ao seu. Contas da AWS A orientação também fornece considerações de design para usar a federação do IAM quando você não pode usar o IAM Identity Center.

Ao trabalhar com funções do IAM para fornecer aos usuários acesso aos AWS recursos, você deve usar o IAM Access Analyzer e o IAM access advisor, conforme descrito nas seções Ferramentas de Segurança e Gerenciamento de Organizações deste guia. Esses serviços ajudam você a obter o mínimo de privilégios, que é um importante controle preventivo que ajuda a criar uma boa postura de segurança.

Considerações sobre design

Para obter o mínimo de privilégios, crie processos para revisar e entender regularmente as relações entre suas identidades e as permissões necessárias para funcionar

adequadamente. Conforme você aprende, ajuste essas permissões e reduza-as gradualmente até o mínimo de permissões possível. Para escalabilidade, essa deve ser uma responsabilidade compartilhada entre suas equipes centrais de segurança e aplicativos. Use recursos como políticas baseadas em recursos, limites de permissão, controles de acesso baseados em atributos e políticas de sessão para ajudar os proprietários de aplicativos a definir um controle de acesso refinado.

Exemplos de implementação

A biblioteca de códigos AWS SRA fornece dois exemplos de implementações que se aplicam a essa fase:

- A política de senha do IAM define a política de senha da conta para que os usuários se alinhem aos padrões de conformidade comuns.
- O Access Analyzer configura um analisador em nível de organização em uma conta de administrador delegado e um analisador em nível de conta em cada conta.

Fase 3: Manter a rastreabilidade

Quando seus usuários tiverem acesso AWS e começarem a criar, você desejará saber quem está fazendo o quê, quando e de onde. Você também desejará visibilidade de possíveis configurações incorretas de segurança, ameaças ou comportamentos inesperados. Uma melhor compreensão das ameaças à segurança permite que você priorize os controles de segurança apropriados. Para monitorar a AWS atividade, siga as recomendações da AWS SRA para configurar uma trilha organizacional usando AWS CloudTraile centralizando seus registros na conta do Log Archive. Para monitoramento de eventos de segurança AWS Security Hub CSPM, use Amazon GuardDuty e Amazon Security Lake conforme descrito na seção de contas do Security Tooling. AWS Config

Considerações sobre design

Ao começar a usar o novo Serviços da AWS, certifique-se de habilitar registros específicos do serviço para o serviço e armazená-los como parte do seu repositório central de registros.

Exemplos de implementação

A biblioteca de códigos AWS SRA fornece os seguintes exemplos de implementações que se aplicam a essa fase:

- CloudTrailA organização cria uma trilha organizacional e define padrões para configurar eventos de dados (por exemplo, no Amazon S3 AWS Lambda e) para reduzir a duplicação CloudTrail do que está configurado por. AWS Control Tower Essa solução fornece opções para configurar eventos de gerenciamento.
- AWS Config A Control Tower Management Account permite que AWS Config a conta de gerenciamento monitore a conformidade dos recursos.
- O Conformance Pack Organization Rules implanta um pacote de conformidade nas contas e regiões especificadas dentro de uma organização.
- AWS Config O Aggregator implanta um agregador delegando a administração a uma conta membro que não seja a conta de auditoria.
- A Security Hub CSPM Organization configura o Security Hub CSPM em uma conta de administrador delegada para as contas e regiões governadas dentro da organização.
- GuardDuty A organização configura GuardDuty dentro de uma conta de administrador delegado para as contas dentro de uma organização.

Fase 4: aplicar segurança em todas as camadas

Neste ponto, você deve ter:

- Os controles de segurança apropriados para o seu Contas da AWS.
- Uma estrutura de conta e UO bem definidas com controles preventivos definidos por meio SCPs de políticas declarativas e funções e políticas do IAM com privilégios mínimos. RCPs
- A capacidade de registrar AWS atividades usando AWS CloudTrail; detectar eventos de segurança usando AWS Security Hub CSPM Amazon GuardDuty e AWS Config; e realizar análises avançadas em um data lake criado especificamente para segurança usando o Amazon Security Lake.

Nesta fase, planeje aplicar a segurança em outras camadas da sua AWS organização, conforme descrito na seção Aplicar serviços de segurança em sua AWS organização. Você pode criar

controles de segurança para sua camada de rede usando serviços como AWS WAF,, AWS Shield, AWS Firewall Manager AWS Network Firewall, AWS Certificate Manager (ACM), Amazon CloudFront, Amazon Route 53 e Amazon VPC, conforme descrito na seção Conta de rede. À medida que você avança na pilha de tecnologia, aplique controles de segurança específicos para sua carga de trabalho ou pilha de aplicativos. Use VPC endpoints, Amazon Inspector,, AWS Systems Manager e AWS Secrets Manager Amazon Cognito conforme descrito na seção Conta do aplicativo.

Considerações sobre design

Ao projetar seus controles de segurança de defesa em profundidade (DiD), considere os fatores de escalabilidade. Sua equipe central de segurança não terá a largura de banda nem o entendimento completo de como cada aplicativo se comporta em seu ambiente. Capacite suas equipes de aplicativos a serem responsáveis por identificar e projetar os controles de segurança corretos para seus aplicativos. A equipe central de segurança deve se concentrar em fornecer as ferramentas e a consultoria certas para capacitar as equipes de aplicativos. Para entender os mecanismos de escalabilidade AWS usados para adotar uma abordagem de segurança mais voltada para a esquerda, consulte a postagem no blog Como AWS construiu o programa Security Guardians, um mecanismo para distribuir a propriedade da segurança.

Exemplos de implementação

A biblioteca de códigos AWS SRA fornece os seguintes exemplos de implementações que se aplicam a essa fase:

- A criptografia padrão do EBS do EC2 configura a criptografia padrão do Amazon EBS no Amazon EC2 para usar o padrão dentro do fornecido. AWS KMS key Regiões da AWS
- O S3 Block Account Public Access configura as configurações de Block Public Access (BPA) em nível de conta no Amazon S3 para contas dentro da organização.
- O Firewall Manager demonstra como configurar uma política e AWS WAF políticas de grupo de segurança para contas dentro de uma organização.
- A Inspector Organization configura o Amazon Inspector em uma conta de administrador delegado para contas e regiões governadas dentro da organização.

Fase 5: Proteja os dados em trânsito e em repouso

Os dados da sua empresa e dos clientes são ativos valiosos que você precisa proteger. AWS fornece vários serviços e recursos de segurança para proteger dados em movimento e em repouso. Use a Amazon CloudFront com AWS Certificate Manager, conforme descrito na seção Conta de rede, para proteger dados em movimento coletados pela Internet. Para dados em movimento em redes internas, use um Application Load Balancer com Autoridade de Certificação Privada da AWS, conforme explicado na seção Conta do aplicativo. AWS KMS e AWS CloudHSM ajudam você a fornecer gerenciamento de chaves criptográficas para proteger os dados em repouso.

Fase 6: Prepare-se para eventos de segurança

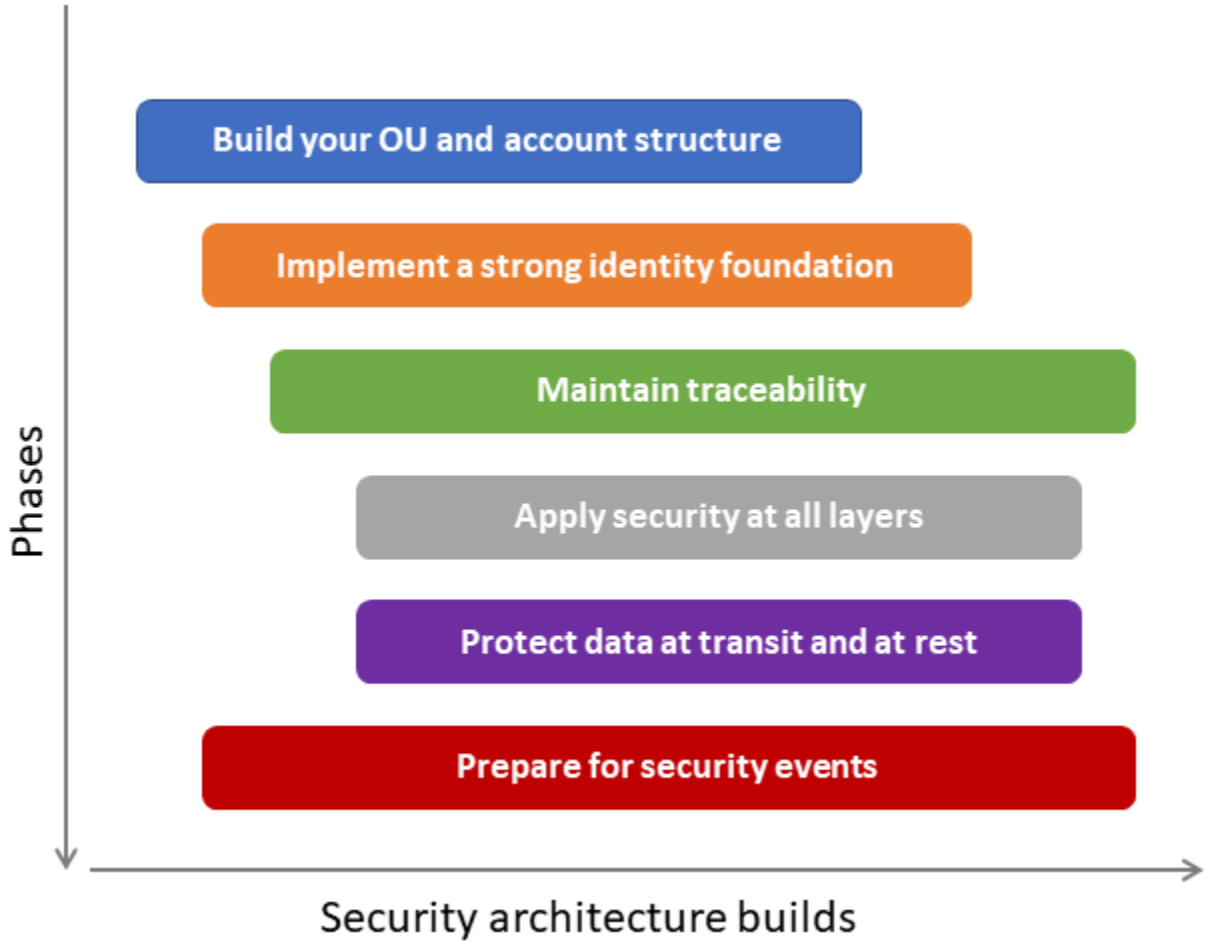
Ao operar seu ambiente de TI, você encontrará eventos de segurança, que são mudanças na operação diária de seu ambiente de TI que indicam uma possível violação da política de segurança ou uma falha no controle de segurança. A rastreabilidade adequada é fundamental para que você esteja ciente de um evento de segurança o mais rápido possível. É igualmente importante estar preparado para fazer a triagem e responder a esses eventos de segurança, para que você possa tomar as medidas adequadas antes que o evento de segurança se intensifique. A preparação ajuda você a fazer uma triagem rápida de um evento de segurança para entender seu impacto potencial.

O AWS SRA, por meio do design da conta do Security Tooling e da implantação de serviços de segurança comuns em todos Contas da AWS, fornece a capacidade de detectar eventos de segurança em toda a organização AWS . O Amazon Detective na conta do Security Tooling ajuda você a fazer a triagem de um evento de segurança e identificar a causa raiz. Durante uma investigação de segurança, você precisa ser capaz de revisar os registros relevantes para registrar e entender o escopo completo e o cronograma do incidente. Os registros também são necessários para a geração de alertas quando ações específicas de interesse acontecem. A AWS SRA recomenda uma conta central de arquivamento de registros para armazenamento imutável de todos os registros operacionais e de segurança. Você pode consultar CloudWatch registros usando o Logs Insights para dados armazenados em grupos de CloudWatch registros e o Amazon Athena e o Amazon OpenSearch Service para dados armazenados no Amazon S3. Use o Amazon Security Lake para centralizar automaticamente os dados de segurança do AWS ambiente, dos provedores de software como serviço (SaaS), locais e de outros provedores de nuvem. Configure assinantes na conta do Security Tooling ou em qualquer conta dedicada, conforme descrito pela AWS SRA, para consultar esses registros para investigação.

AWS Security Incident Responseajuda você a automatizar a resposta, a investigação e a remediação de incidentes de segurança. Ele fornece playbooks e fluxos de trabalho predefinidos para ajudá-lo a responder aos eventos de segurança de forma rápida e consistente. Quando o recurso de resposta proativa está ativado, o Security Incident Response se integra ao Security Hub CSPM e GuardDuty aciona automaticamente fluxos de trabalho de resposta quando descobertas de segurança são detectadas. O serviço ajuda você a padronizar e automatizar seus processos de resposta a incidentes em toda a organização. AWS Se precisar de assistência adicional, você pode abrir um caso com suporte de serviço para entrar em contato com a Equipe de Resposta a Incidentes AWS do Cliente (CIRT).

Considerações sobre design

- Você deve começar a se preparar para detectar e responder aos eventos de segurança desde o início de sua jornada na nuvem. Para melhor utilizar os recursos limitados, atribua dados e a importância dos negócios aos seus AWS recursos para que, ao detectar um evento de segurança, você possa priorizar a triagem e a resposta com base na criticidade dos recursos envolvidos.
- As fases para criar sua arquitetura de segurança na nuvem, conforme discutido nesta seção, são de natureza sequencial. No entanto, você não precisa esperar pela conclusão completa de uma fase antes de iniciar a próxima. Recomendamos que você adote uma abordagem iterativa, na qual comece a trabalhar em várias fases paralelamente e evolua cada fase à medida que evolui sua postura de segurança na nuvem. Conforme você passa pelas diferentes fases, seu design evolui. Considere adaptar a sequência sugerida mostrada no diagrama a seguir de acordo com suas necessidades específicas.



Exemplo de implementação

A biblioteca de códigos da AWS SRA fornece um exemplo de implementação de uma organização de detetives, que habilita automaticamente o Amazon Detective delegando a administração a uma conta (por exemplo, ferramentas de auditoria ou segurança) e configura o Detective para contas existentes e futuras. AWS Organizations

AWS Lista de verificação das melhores práticas da SRA

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Esta seção resume as melhores práticas de AWS SRA detalhadas ao longo deste guia em uma lista de verificação que você pode seguir ao criar sua versão da arquitetura de segurança. AWS Use essa lista como um ponto de referência e não como um substituto para revisar o guia. A lista de verificação é agrupada por. AWS service (Serviço da AWS)Se você quiser validar programaticamente seu AWS ambiente existente em relação à lista de verificação de melhores práticas da AWS SRA, você pode usar o SRA Verify.

O SRA Verify é uma ferramenta de avaliação de segurança que ajuda você a avaliar o alinhamento da sua organização com o AWS SRA em várias Contas da AWS regiões. Ele mapeia diretamente as recomendações da AWS SRA, fornecendo verificações automatizadas que validam sua implementação de acordo com a orientação da AWS SRA. A ferramenta ajuda você a verificar se seus serviços de segurança estão configurados corretamente de acordo com a arquitetura de referência. Ele fornece descobertas detalhadas e etapas de remediação acionáveis para ajudar a garantir que seu AWS ambiente siga as melhores práticas de segurança. O SRA Verify foi projetado para ser executado AWS CodeBuild na conta de auditoria da organização (Ferramentas de Segurança). Você também pode executá-lo localmente ou estendê-lo usando a biblioteca SRA Verify.

> **Note**
>
> O SRA Verify contém verificações para vários serviços, mas pode não conter uma verificação para todas as considerações do AWS SRA. Para obter mais informações, consulte os guias na biblioteca da AWS SRA.

AWS Organizations

- AWS Organizations está habilitado com todos os recursos.
- As políticas de controle de serviço (SCPs) são usadas para definir diretrizes de controle de acesso para diretores do IAM.

- As políticas de controle de recursos (RCPs) são usadas para definir diretrizes de controle de acesso para AWS recursos.
- As políticas declarativas são usadas para declarar e aplicar centralmente a configuração desejada para uma determinada escala AWS service (Serviço da AWS) em toda a organização.
- Três contas básicas OUs são criadas (segurança, infraestrutura e carga de trabalho) para agrupar contas de membros que fornecem serviços básicos.
- A conta do Security Tooling é criada na OU de Segurança. Essa conta fornece gerenciamento centralizado de serviços de AWS segurança e outras ferramentas de segurança de terceiros.
- A conta do Log Archive é criada na OU de Segurança. Essa conta fornece um repositório central de registros Serviços da AWS e registros de aplicativos rigidamente controlados.
- A conta de rede é criada na UO de Infraestrutura. Essa conta gerencia o gateway entre seu aplicativo e a Internet em geral. Ele isola os serviços de rede, a configuração e a operação das cargas de trabalho de aplicativos individuais, da segurança e de outras infraestruturas.
- A conta do Shared Service é criada na UO de Infraestrutura. Essa conta oferece suporte aos serviços que vários aplicativos e equipes usam para fornecer seus resultados.
- A conta do aplicativo é criada na OU de cargas de trabalho. Essa conta hospeda a infraestrutura e os serviços principais para executar e manter um aplicativo corporativo. Este guia fornece uma representação, mas no mundo real, haverá várias OUs contas de membros segregadas por aplicativos, ambientes de desenvolvimento e outras considerações de segurança.
- Informações de contato alternativas para cobrança, operações e segurança de todas as contas dos membros estão configuradas.

AWS CloudTrail

- Uma trilha da organização é configurada para permitir a entrega de eventos de CloudTrail gerenciamento na conta de gerenciamento e em todas as contas de membros em uma AWS organização.
- A trilha da organização é configurada como trilha multirregional.
- A trilha da organização está configurada para capturar eventos de recursos globais.
- Trilhas adicionais para capturar eventos de dados específicos são configuradas conforme necessário para monitorar atividades confidenciais AWS de recursos.
- A conta do Security Tooling é definida como administrador delegado da trilha da organização.

- A trilha da organização está configurada para ser ativada automaticamente para todas as novas contas de membros.
- A trilha da organização está configurada para publicar registros em um bucket S3 centralizado hospedado na conta do Log Archive.
- A trilha da organização tem a validação do arquivo de log habilitada para verificar a integridade dos arquivos de log.
- A trilha da organização é integrada aos CloudWatch registros para retenção de registros.
- A trilha da organização é criptografada usando uma chave gerenciada pelo cliente.
- O bucket central do S3 usado para o repositório de registros na conta do Log Archive é criptografado com uma chave gerenciada pelo cliente.
- O bucket central do S3 usado para o repositório de registros na conta do Log Archive é configurado com o S3 Object Lock para imutabilidade.
- O controle de versão está habilitado para o bucket central do S3 que é usado para o repositório de registros na conta do Log Archive.
- O bucket central do S3 usado para o repositório de registros na conta do Log Archive tem uma política de recursos definida que restringe o upload de objetos somente pela trilha da organização por meio do recurso Amazon Resource Name (ARN).

AWS Security Hub CSPM

- O CSPM do Security Hub está habilitado para todas as contas de membros e para a conta de gerenciamento.
- AWS Config está habilitado para todas as contas de membros como pré-requisito para o CSPM do Security Hub.
- A conta do Security Tooling é definida como administrador delegado do Security Hub CSPM.
- A Amazon GuardDuty e o Amazon Detective têm a mesma conta de administrador delegado do Security Hub CSPM para facilitar a integração dos serviços.
- A configuração central é usada para configurar e gerenciar o CSPM do Security Hub em vários e. Contas da AWS Regiões da AWS
- Todas as contas da OU e dos membros são designadas como gerenciadas centralmente pelo administrador delegado do Security Hub CSPM.
- O CSPM do Security Hub é ativado automaticamente para todas as novas contas de membros.
- O Security Hub CSPM é habilitado automaticamente para configuração de novos padrões.

- As descobertas do CSPM do Security Hub de todas as regiões são agregadas em uma única região de origem.
- As descobertas do CSPM do Security Hub de todas as contas dos membros são agregadas na conta do Security Tooling.
- O padrão AWS Foundational Best Practices (FSBP) no Security Hub CSPM está habilitado para todas as contas dos membros.
- O padrão CIS AWS Foundation Benchmark no Security Hub CSPM está habilitado para todas as contas dos membros.
- Outros padrões CSPM do Security Hub são habilitados conforme aplicável.
- Uma regra de automação CSPM do Security Hub é usada para enriquecer as descobertas com o contexto dos recursos.
- O recurso automatizado de resposta e remediação do Security Hub CSPM é usado para criar EventBridge regras personalizadas para realizar ações automáticas em relação a descobertas específicas.

AWS Config

- O AWS Config gravador está habilitado para todas as contas de membros e para a conta de gerenciamento.
- O AWS Config gravador está habilitado para todas as regiões.
- O bucket S3 do canal de AWS Config entrega está centralizado na conta do Log Archive.
- A conta do administrador AWS Config delegado é definida como a conta do Security Tooling.
- AWS Config tem um agregador organizacional configurado. O agregador inclui todas as regiões.
- AWS Config os pacotes de conformidade são implantados uniformemente em todas as contas dos membros a partir da conta de administrador delegado.
- AWS Config as descobertas das regras são enviadas automaticamente para o CSPM do Security Hub.

Amazon GuardDuty

- GuardDuty O detector está ativado para todas as contas de membros e para a conta de gerenciamento.

- GuardDuty O detector está habilitado para todas as regiões.
- GuardDuty O detector é ativado automaticamente para todas as novas contas de membros.
- GuardDuty a administração delegada é definida na conta do Security Tooling.
- GuardDuty fontes de dados fundamentais, como eventos CloudTrail de gerenciamento, registros de fluxo de VPC e registros de consulta de DNS do Route 53 Resolver, estão habilitadas.
- GuardDuty A Proteção S3 está ativada.
- GuardDuty A proteção contra malware para volumes do EBS está ativada.
- GuardDuty A proteção contra malware para S3 está ativada.
- GuardDuty A Proteção RDS está ativada.
- GuardDuty A Proteção Lambda está ativada.
- GuardDuty A Proteção EKS está ativada.
- GuardDuty O EKS Runtime Monitoring está ativado.
- GuardDuty A detecção estendida de ameaças está ativada.
- GuardDuty as descobertas são exportadas para um bucket central do S3 na conta do Log Archive para retenção.

IAM

- Os usuários do IAM não são usados.
- O gerenciamento centralizado do acesso root às contas dos membros é imposto.
- A tarefa centralizada de usuário raiz privilegiado para a conta de gerenciamento é imposta pelo administrador delegado.
- O gerenciamento centralizado do acesso raiz é delegado à conta do Security Tooling.
- Todas as credenciais raiz da conta do membro são removidas.
- Todas as políticas de Conta da AWS senha para membros e gerentes são definidas de acordo com o padrão de segurança da organização.
- O consultor de acesso do IAM é usado para revisar as últimas informações usadas para grupos, usuários, funções e políticas do IAM.
- Os limites de permissão são usados para restringir o máximo possível de permissões para funções do IAM.

IAM Access Analyzer

- O IAM Access Analyzer está habilitado para todas as contas de membros e para a conta de gerenciamento.
- O administrador delegado do IAM Access Analyzer está configurado para a conta do Security Tooling.
- O analisador de acesso externo do IAM Access Analyzer é configurado com a zona de confiança da organização em cada região.
- O analisador de acesso externo do IAM Access Analyzer é configurado com a zona de confiança da conta em cada região.
- O analisador de acesso interno do IAM Access Analyzer é configurado com a zona de confiança da organização em cada região.
- O analisador de acesso interno do IAM Access Analyzer é configurado com a zona de confiança da conta em cada região.
- O analisador de acesso não utilizado do IAM Access Analyzer para a conta atual é criado.
- O analisador de acesso não utilizado do IAM Access Analyzer para a organização atual é criado.

Amazon Detective

- Detective está habilitado para todas as contas de membros.
- Detective é ativado automaticamente para todas as novas contas de membros.
- Detective está habilitado para todas as regiões.
- O administrador delegado do Detective está configurado para a conta do Security Tooling.
- O administrador delegado do Detective e do Security Hub CSPM está configurado para a mesma conta do Security Tooling. GuardDuty
- O Detective é integrado ao Security Lake para armazenamento e análise de registros brutos.
- O Detective é integrado GuardDuty para ingerir as descobertas.
- Detective está ingerindo registros de auditoria do Amazon EKS para análise.
- Detective está ingerindo registros CSPM do Security Hub para análise.

AWS Firewall Manager

- As políticas de segurança do Firewall Manager estão definidas.
- O administrador delegado do Firewall Manager está configurado para a conta do Security Tooling.
- AWS Config é habilitado como pré-requisito.
- Vários administradores do Firewall Manager estão configurados com escopo restrito por UO, conta e região.
- Uma política de AWS WAF segurança do Firewall Manager é definida.
- Uma política de registro AWS WAF centralizada do Firewall Manager é definida.
- Uma política de segurança do Firewall Manager Shield Advanced é definida.
- Uma política de segurança do grupo de segurança do Firewall Manager está definida.

Amazon Inspector

- O Amazon Inspector está habilitado para todas as contas dos membros.
- O Amazon Inspector é habilitado automaticamente para qualquer nova conta de membro.
- O administrador delegado do Amazon Inspector está configurado para a conta do Security Tooling.
- A verificação de EC2 vulnerabilidades do Amazon Inspector está ativada.
- O escaneamento de vulnerabilidade de imagem ECR do Amazon Inspector está ativado.
- A função Amazon Inspector Lambda e a verificação de vulnerabilidades de camadas estão habilitadas.
- A digitalização de código do Amazon Inspector Lambda está ativada.
- A verificação de segurança do código do Amazon Inspector está ativada.

Amazon Macie

- O Macie está habilitado para contas de membros aplicáveis.
- O Macie é ativado automaticamente para novas contas de membros aplicáveis.
- O administrador delegado do Macie está configurado para a conta do Security Tooling.
- As descobertas do Macie são exportadas para um bucket central do S3 na conta do log Archive.

- Os buckets do S3 que armazenam as descobertas do Macie são criptografados com uma chave gerenciada pelo cliente.
- A política e a política de classificação do Macie são publicadas no Security Hub CSPM.

Amazon Security Lake

- A configuração da organização do Security Lake está ativada.
- O administrador delegado do Security Lake está configurado para a conta do Security Tooling.
- A configuração da organização Security Lake está habilitada para novas contas de membros.
- A conta do Security Tooling é configurada como assinante de acesso a dados para realizar análises de registros.
- A conta do Security Tooling é configurada como assinante de consulta de dados para realizar análises de registros.
- Uma fonte CloudTrail de registro de gerenciamento está habilitada para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- Uma fonte de log de fluxo de VPC está habilitada para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- Uma fonte de log do Route 53 está habilitada para o Security Lake em todas as contas de membros ativos ou em determinadas contas de membros.
- CloudTrail o evento de dados de uma fonte de log do S3 está habilitado para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- Uma fonte de log de execução do Lambda está habilitada para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- Uma fonte de log de auditoria do Amazon EKS está habilitada para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- Uma fonte de registro de descobertas do Security Hub está habilitada para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- Uma fonte de AWS WAF log está habilitada para o Security Lake em todas as contas de membros ativas ou em determinadas contas de membros.
- As filas SQS do Security Lake na conta do administrador delegado são criptografadas com uma chave gerenciada pelo cliente.
- A fila de mensagens mortas do Security Lake SQS na conta do administrador delegado é criptografada com uma chave gerenciada pelo cliente.

- O bucket do Security Lake S3 é criptografado com uma chave gerenciada pelo cliente.
- O bucket do Security Lake S3 tem uma política de recursos que restringe o acesso direto somente pelo Security Lake.

AWS WAF

- Todas as CloudFront distribuições estão associadas a. AWS WAF
- Todos os REST do Amazon API Gateway APIs estão associados AWS WAF a.
- Todos os balanceadores de carga de aplicativos estão associados a. AWS WAF
- Todos os AWS AppSync GraphQL APIs estão associados a. AWS WAF
- Todos os grupos de usuários do Amazon Cognito estão associados a. AWS WAF
- Todos os AWS App Runner serviços estão associados AWS WAF a.
- Todas as Acesso Verificado pela AWS instâncias estão associadas AWS WAF a.
- Todos os AWS Amplify aplicativos estão associados AWS WAF a.
- AWS WAF o registro está ativado.
- AWS WAF os registros são centralizados em um bucket do S3 na conta do Log Archive.

AWS Shield Advanced

- A assinatura do Shield Advanced está ativada e configurada para renovação automática para todas as contas de aplicativos que tenham recursos voltados para o público.
- O Shield Advanced está configurado para todas as CloudFront distribuições.
- O Shield Advanced está configurado para todos os Application Load Balancers.
- O Shield Advanced está configurado para todos os balanceadores de carga de rede.
- O Shield Advanced está configurado para todas as zonas hospedadas do Route 53.
- O Shield Advanced está configurado para todos os endereços IP elásticos.
- O Shield Advanced está configurado para todos os aceleradores globais.
- CloudWatch os alarmes são CloudFront configurados para recursos do Route 53 protegidos pelo Shield Advanced.
- O acesso ao Shield Response Team (SRT) está configurado.
- O engajamento proativo do Shield Advanced está ativado.

- Os contatos de engajamento proativo do Shield Advanced estão configurados.
- Os recursos protegidos do Shield Advanced têm uma AWS WAF regra personalizada configurada.
- Os recursos protegidos do Shield Advanced têm a mitigação automática da camada de aplicação DDo S ativada.

AWS Resposta a incidentes de segurança

- AWS O Security Incident Response está habilitado para toda a AWS organização.
- O administrador delegado do AWS Security Incident Response está configurado para a conta do Security Tooling.
- O fluxo de trabalho proativo de resposta e triagem de alertas está ativado.
- AWS As ações de contenção da Equipe de Resposta a Incidentes do Cliente (CIRT) são autorizadas.

AWS Audit Manager

- O Audit Manager está habilitado para todas as contas dos membros.
- O Audit Manager é ativado automaticamente para novas contas de membros.
- O administrador delegado do Audit Manager está configurado para a conta do Security Tooling.
- AWS Config está habilitado como pré-requisito para o Audit Manager.
- Uma chave gerenciada pelo cliente é usada para dados armazenados no Audit Manager.
- O destino padrão do relatório de avaliação está configurado.

Recursos do IAM

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Embora o AWS Identity and Access Management (IAM) não seja um serviço incluído em um diagrama de arquitetura tradicional, ele abrange todos os aspectos da AWS organização Contas da AWS, e. Serviços da AWS Você não pode implantar nenhuma Serviços da AWS sem primeiro criar entidades do IAM e conceder permissões. Uma explicação completa do IAM está além do escopo deste documento, mas esta seção fornece resumos importantes das recomendações de melhores práticas e dicas para recursos adicionais.

- Para conhecer as melhores práticas do IAM, consulte as melhores práticas de segurança no IAM na AWS documentação, os artigos do IAM no blog de AWS segurança e as apresentações do AWS re:Invent.
- O pilar de segurança AWS Well-Architected descreve as principais etapas do processo de gerenciamento de permissões: definir barreiras de permissões, conceder acesso com privilégios mínimos, analisar o acesso público e entre contas, compartilhar recursos com segurança, reduzir as permissões continuamente e estabelecer um processo de acesso de emergência.
- A tabela a seguir e as notas anexas fornecem uma visão geral de alto nível da orientação recomendada sobre os tipos de políticas de permissão do IAM disponíveis e como usá-las em sua arquitetura de segurança. Para saber mais, assista ao vídeo do AWS re:Invent 2020 sobre como escolher a combinação certa de políticas de IAM.

Caso de uso ou política	Efeito	Gerenciado por	Finalidade	Pertence a	Afeta	Implantado em
Políticas de controle de serviços (SCPs)	Restrict	Equipe central, como plataforma ou	Guardrails, governança	Organização, OU, conta	Todos os diretores em organizaç	Conta de gerenciamento da organização [2]

		equipe de segurança [1]			ão, OU e contas	
Políticas de controle de recursos (RCPs)	Restrict	Equipe central, como plataforma ou equipe de segurança [1]	Guardrails, governança	Organização, OU, conta	Recursos nas contas dos membros [12]	Conta de gerenciamento da organização [2]
Políticas básicas de automação de contas (as funções do IAM usadas pela plataforma para operar uma conta)	Conceder e restringir	Equipe central, como plataforma, segurança ou equipe do IAM [1]	Permissões para funções (básicas) que não sejam de automação de carga de trabalho [3]	Conta única [4]	Princípios usados pela automação em uma conta de membro	Contas-membros

Políticas humanas básicas (as funções do IAM que concedem aos usuários permissões para realizar seu trabalho)	Conceder e restringir	Equipe central, como plataforma, segurança ou equipe do IAM [1]	Permissões para funções humanas [5]	Conta única [4]	Diretores federados [5] e usuários do IAM [6]	Contas-membros
Limites de permissões (permissões máximas que um desenvolvedor capacitado pode atribuir a outro diretor)	Restrict	Equipe central, como plataforma, segurança ou equipe do IAM [1]	Guardrails para funções de candidatura (devem ser aplicados)	Conta única [4]	Funções individuais para um aplicativo ou carga de trabalho nessa conta [7]	Contas-membros

Políticas de função de máquina para aplicativos (função associada à infraestrutura implantada por desenvolvedores)	Conceder e restringir	Delegado aos desenvolvedores [8]	Permissão para o aplicativo ou carga de trabalho [9]	Conta única	Um principal nesta conta	Contas-membros
Políticas de recursos	Conceder e restringir	Delegado aos desenvolvedores [8,10]	Permissões para recursos	Conta única	Um principal em uma conta [11]	Contas-membros
Gerenciamento central de usuários raiz	Conceder e restringir	Equipe central, como plataforma, segurança ou equipe do IAM [1]	Gerencie centralmente os usuários raiz da conta do membro em grande escala	Organização	Todos os usuários root nas contas dos membros	Conta de gerenciamento da organização, conta de administrador delegado

Notas da tabela:

1. As empresas têm muitas equipes centralizadas (como plataforma em nuvem, operações de segurança ou equipes de gerenciamento de identidade e acesso) que dividem as responsabilidades desses controles independentes e revisam as políticas umas das outras. Os

exemplos na tabela são espaços reservados. Você precisará determinar a separação de tarefas mais eficaz para sua empresa.

2. Para usar SCPs, você deve habilitar todos os recursos contidos no AWS Organizations.
3. Geralmente, são necessárias funções e políticas básicas comuns para permitir a automação, como permissões para o pipeline, ferramentas de implantação, ferramentas de monitoramento (por exemplo, AWS Lambda e Regras do AWS Config) e outras permissões. Essa configuração geralmente é fornecida quando a conta é provisionada.
4. Embora pertençam a um recurso (como uma função ou política) em uma única conta, eles podem ser replicados ou implantados em várias contas usando. AWS CloudFormation StackSets
5. Defina um conjunto básico de funções e políticas humanas básicas que são implantadas em todas as contas dos membros por uma equipe central (geralmente durante o provisionamento da conta). Os exemplos incluem os desenvolvedores da equipe da plataforma, a equipe do IAM e as equipes de auditoria de segurança.
6. Use a federação de identidades (em vez de usuários locais do IAM) sempre que possível.
7. Os limites de permissões são usados por administradores delegados. Essa política do IAM define as permissões máximas e substitui outras políticas (incluindo `"*:*"` políticas que permitem todas as ações nos recursos). Os limites de permissões devem ser exigidos nas políticas humanas básicas como condição para criar funções (como funções de desempenho da carga de trabalho) e anexar políticas. Configurações adicionais, como SCPs impor a anexação do limite de permissões.
8. Isso pressupõe que grades de proteção suficientes (por exemplo, SCPs e limites de permissões) tenham sido implantadas.
9. Essas políticas opcionais podem ser fornecidas durante o provisionamento da conta ou como parte do processo de desenvolvimento do aplicativo. A permissão para criar e anexar essas políticas será regida pelas próprias permissões do desenvolvedor do aplicativo.
10. Além das permissões da conta local, uma equipe centralizada (como a equipe da plataforma em nuvem ou a equipe de operações de segurança) geralmente gerencia algumas políticas baseadas em recursos para permitir o acesso entre contas para operar as contas (por exemplo, para fornecer acesso aos buckets do S3 para registro).
11. Uma política de IAM baseada em recursos pode se referir a qualquer principal em qualquer conta para permitir ou negar acesso a seus recursos. Pode até se referir a diretores anônimos para permitir o acesso público.

12RCPs aplicam-se aos recursos de um subconjunto de. Serviços da AWS Para obter mais informações, consulte Lista Serviços da AWS desse suporte RCPs na AWS Organizations documentação.

Garantir que as identidades do IAM tenham apenas as permissões necessárias para um conjunto bem delineado de tarefas é fundamental para reduzir o risco de abuso malicioso ou não intencional de permissões. Estabelecer e manter um modelo de privilégio mínimo exige um plano deliberado para atualizar, avaliar e mitigar continuamente o excesso de privilégios. Aqui estão algumas recomendações adicionais para esse plano:

- Use o modelo de governança da sua organização e o apetite estabelecido pelo risco para estabelecer barreiras e limites de permissões específicos.
- Implemente o menor privilégio por meio de um processo continuamente iterativo. Este não é um exercício único.
- Use SCPs para reduzir o risco acionável. Pretende-se que sejam amplas barreiras de proteção, não controles restritos.
- Use limites de permissões para delegar a administração do IAM de forma mais segura.
  - Certifique-se de que os administradores delegados anexem a política de limite do IAM apropriada às funções e aos usuários que eles criam.
- Como defense-in-depth abordagem (em conjunto com políticas baseadas em identidade), use políticas de IAM baseadas em recursos para negar amplo acesso aos recursos.
- Use o consultor de acesso do IAM AWS CloudTrail, o IAM Access Analyzer e as ferramentas relacionadas para analisar regularmente o uso histórico e as permissões concedidas. Corrija imediatamente as permissões excessivas óbvias.
- Defina ações amplas para recursos específicos, quando aplicável, em vez de usar um asterisco como curinga para indicar todos os recursos.
- Implemente um mecanismo para identificar, analisar e aprovar rapidamente as exceções da política do IAM com base nas solicitações.

Repositório de código para exemplos de AWS SRA

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Para ajudar você a começar a criar e implementar a orientação no AWS SRA, um repositório de infraestrutura como código (IaC) em https://github.com/aws-samples/aws-security-reference-architecture-examples acompanha este guia. Esse repositório contém código para ajudar desenvolvedores e engenheiros a implantar alguns dos padrões de orientação e arquitetura apresentados neste documento. Esse código foi extraído da experiência em primeira mão dos consultores de Serviços AWS Profissionais com os clientes. Os modelos são de natureza geral — seu objetivo é ilustrar um padrão de implementação em vez de fornecer uma solução completa. As AWS service (Serviço da AWS) configurações e as implantações de recursos são deliberadamente muito restritivas. Talvez seja necessário modificar e adaptar essas soluções para atender às suas necessidades de ambiente e segurança.

O repositório de código AWS SRA fornece exemplos de código com ambas as opções de implantação AWS CloudFormation e do Terraform. Os padrões de solução oferecem suporte a dois ambientes: um requer AWS Control Tower e o outro usa AWS Organizations sem AWS Control Tower. As soluções necessárias neste repositório AWS Control Tower foram implantadas e testadas em um AWS Control Tower ambiente usando AWS CloudFormation e personalizações para AWS Control Tower (cFct). As soluções que não exigem AWS Control Tower foram testadas em um AWS Organizations ambiente usando AWS CloudFormation. A solução cFct ajuda os clientes a configurar rapidamente um AWS ambiente seguro com várias contas com base nas AWS melhores práticas. Isso ajuda a economizar tempo automatizando a configuração de um ambiente para executar cargas de trabalho seguras e escaláveis, ao mesmo tempo em que implementa uma linha de base de segurança inicial por meio da criação de contas e recursos. AWS Control Tower também fornece um ambiente básico para começar com uma arquitetura de várias contas, gerenciamento de identidade e acesso, governança, segurança de dados, design de rede e registro. As soluções no repositório AWS SRA fornecem configurações de segurança adicionais para implementar os padrões descritos neste documento.

Aqui está um resumo das soluções no repositório AWS SRA. Cada solução inclui um `README.md` arquivo com detalhes.

- A solução CloudTrail Organização cria uma trilha organizacional na conta de gerenciamento da organização e delega a administração a uma conta de membro, como a conta de ferramentas de auditoria ou segurança. Essa trilha é criptografada com uma chave gerenciada pelo cliente criada na conta do Security Tooling e entrega os registros para um bucket do S3 na conta do Log Archive. Opcionalmente, os eventos de dados podem ser habilitados para o Amazon S3 AWS Lambda e suas funções. Uma trilha da organização registra eventos para todos Contas da AWS na AWS organização, evitando que as contas dos membros modifiquem as configurações.
- A solução GuardDuty Organization habilita a Amazon GuardDuty delegando a administração à conta do Security Tooling. Ele é configurado GuardDuty na conta do Security Tooling para todas as contas existentes e futuras AWS da organização. As GuardDuty descobertas também são criptografadas com uma chave KMS e enviadas para um bucket do S3 na conta do Log Archive.
- A solução Security Hub CSPM Organization configura o CSPM do Security Hub delegando a administração à conta do Security Tooling. Ele configura o CSPM do Security Hub na conta do Security Tooling para todas as contas existentes e futuras da organização. AWS A solução também fornece parâmetros para sincronizar os padrões de segurança habilitados em todas as contas e regiões, bem como configurar um agregador de regiões na conta do Security Tooling. A centralização do CSPM do Security Hub na conta do Security Tooling fornece uma visão cruzada da conformidade com os padrões de segurança e das descobertas de integrações e de terceiros. Serviços da AWS AWS Partner
- A solução Inspector configura o Amazon Inspector dentro da conta de administrador delegado (Security Tooling) para todas as contas e regiões governadas da organização. AWS
- A solução Firewall Manager configura as políticas AWS Firewall Manager de segurança delegando a administração à conta do Security Tooling e configurando o Firewall Manager com uma política de grupo de segurança e várias políticas. AWS WAF A política de grupo de segurança exige um grupo de segurança máximo permitido em uma VPC (existente ou criada pela solução), que é implantada pela solução.
- A solução Macie Organization habilita o Amazon Macie delegando a administração à conta do Security Tooling. Ele configura o Macie na conta do Security Tooling para todas as contas existentes e futuras AWS da organização. O Macie está ainda configurado para enviar seus resultados de descoberta para um bucket central do S3 que é criptografado com uma chave KMS.
- AWS Config:
  - A solução Config Aggregator configura um AWS Config agregador delegando a administração à conta do Security Tooling. Em seguida, a solução configura um AWS Config agregador na conta do Security Tooling para todas as contas existentes e futuras na organização. AWS

  - A solução Conformance Pack Organization Rules é Regras do AWS Config implantada delegando a administração à conta do Security Tooling. Em seguida, ele cria um pacote de conformidade organizacional dentro da conta de administrador delegado para todas as contas existentes e futuras na organização. AWS A solução está configurada para implantar o modelo de amostra de pacote de conformidade com as melhores práticas operacionais para criptografia e gerenciamento de chaves.
  - A solução AWS Config Control Tower Management Account ativa AWS Config a conta AWS Control Tower de gerenciamento e atualiza adequadamente o AWS Config agregador na conta do Security Tooling. A solução usa o AWS Control Tower CloudFormation modelo de habilitação AWS Config como referência para garantir a consistência com as outras contas na AWS organização.
- IAM:
  - A solução Access Analyzer habilita o IAM Access Analyzer delegando a administração à conta do Security Tooling. Em seguida, ele configura um analisador de acesso IAM em nível organizacional dentro da conta do Security Tooling para todas as contas existentes e futuras na organização. AWS A solução também implanta o IAM Access Analyzer em todas as contas e regiões membros para apoiar a análise de permissões em nível de conta.
  - A solução IAM Password Policy atualiza a política de Conta da AWS senhas em todas as contas de uma AWS organização. A solução fornece parâmetros para definir as configurações da política de senha para ajudá-lo a se alinhar aos padrões de conformidade do setor.
- A solução de criptografia EC2 padrão do EBS permite a criptografia padrão do Amazon EBS em nível de conta dentro de cada conta Conta da AWS e Região da AWS dentro da organização. AWS Ele impõe a criptografia dos novos volumes e snapshots do EBS que você cria. Por exemplo, o Amazon EBS criptografa os volumes do EBS que são criados quando você executa uma instância e os snapshots que você copia de um snapshot não criptografado.
- A solução S3 Block Account Public Access permite configurações em nível de conta do Amazon S3 em cada uma na Conta da AWS organização. AWS O recurso Bloqueio de acesso público do Amazon S3 fornece configurações para pontos de acesso, buckets e contas para ajudar você a gerenciar o acesso público aos recursos do Amazon S3. Por padrão, novos buckets, pontos de acesso e objetos não permitem acesso público. No entanto, os usuários podem modificar políticas de bucket, políticas de ponto de acesso ou permissões de objeto para permitir acesso público. As configurações do Amazon S3 Block Public Access substituem essas políticas e permissões para que você possa limitar o acesso público a esses recursos.

- A solução Detective Organization automatiza a habilitação do Amazon Detective delegando a administração a uma conta (como a conta Audit ou Security Tooling) e configurando o Detective para todas as contas existentes e futuras. AWS Organizations
- A solução Shield Advanced automatiza a implantação do AWS Shield Advanced para fornecer proteção DDo S aprimorada para seus aplicativos em AWS.
- A solução AMI Bakery Organization ajuda a automatizar o processo de criação e gerenciamento de imagens padrão e reforçadas da Amazon Machine Image (AMI). Isso garante consistência e segurança em todas as suas AWS instâncias e simplifica as tarefas de implantação e manutenção.
- A solução Patch Manager ajuda a simplificar o gerenciamento de patches em vários Contas da AWS. Você pode usar essa solução para atualizar o AWS Systems Manager Agente (Agente SSM) em todas as instâncias gerenciadas e para verificar e instalar patches de segurança e correções de erros críticos e importantes em instâncias marcadas do Windows e do Linux. A solução também configura a configuração padrão de gerenciamento de host para detectar a criação de novas Contas da AWS e implantar automaticamente a solução nessas contas.

Colaboradores

Autor principal:

- Avik Mukherjee, Segurança Sênior da SA AWS

Colaboradores:

- Jason Hurst, investigador sênior de segurança AWS do CIRT
- Abhishek Panday, gerente de produto AWS principal — Tecnologia
- Itay Meller, especialista AWS sênior em SA
- Jonathan VanKim, AWS diretor de segurança da SA
- Josh Du Lac, estrategista de segurança AWS corporativa
- James Thompson, arquiteto AWS sênior de soluções
- Jeremy Girven, especialista em SA AWS
- Rodney Underkoffler, especialista sênior em SA AWS
- Farhan Farooq, AWS arquiteto sênior de soluções
- Prashob Krishnan, gerente técnico de contas AWS
- Meg Peddada, consultora AWS sênior de segurança
- Ashwin Phadke, AWS arquiteto sênior de soluções
- Sowjanya Rajavaram, Segurança Sênior SA AWS
- Tomek Jakubowski, consultor sênior AWS
- Arun Thomas, arquiteto AWS sênior de soluções
- Ross Warren, arquiteto de soluções de AWS produtos
- Scott Conklin, consultor sênior AWS
- Ilya Epshteyn, gerente AWS sênior de soluções de identidade
- Michael Haken, tecnólogo AWS principal
- Mehial Mendrin, consultor sênior AWS
- Christopher Evensen, gerente técnico AWS sênior de contas

Analisando:

- Eric Rose, AWS diretor de segurança da SA
- Manoj Kumar, AWS consultor de entrega

Redação técnica:

- Handan Selamoglu, redator técnico sênior AWS

Apêndice: serviços AWS de segurança, identidade e conformidade

Influencie o futuro da Arquitetura de Referência de AWS Segurança (AWS SRA) respondendo a uma breve pesquisa.

Para uma introdução ou uma atualização, consulte Segurança, identidade e conformidade AWS no AWS site para obter uma lista dos Serviços da AWS que ajudam você a proteger suas cargas de trabalho e aplicativos na nuvem. Esses serviços são agrupados em cinco categorias: proteção de dados, gerenciamento de identidade e acesso, proteção de rede e aplicativos, detecção de ameaças e monitoramento contínuo e conformidade e privacidade de dados.

Proteção de dados — AWS fornece serviços que ajudam você a proteger seus dados, contas e cargas de trabalho contra acesso não autorizado.

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

Gerenciamento de identidade e acesso — os serviços de AWS identidade permitem que você gerencie com segurança identidades, recursos e permissões em grande escala.

- IAM — controle com segurança o acesso Serviços da AWS e os recursos.
- IAM Identity Center — gerencie centralmente o acesso por SSO a vários Contas da AWS aplicativos comerciais.
- Amazon Cognito — Adicione cadastro, login e controle de acesso de usuários aos seus aplicativos web e móveis.

- AWS Directory Service— Use o Microsoft Active Directory gerenciado no Nuvem AWS.
- AWS RAM— Compartilhe AWS recursos de forma simples e segura.
- AWS Organizations— implemente o gerenciamento baseado em políticas para vários. Contas da AWS
- Permissões verificadas pela Amazon — Gerencie permissões e autorizações escaláveis e refinadas em seus aplicativos personalizados.

Proteção de rede e aplicativos — Essas categorias de serviços permitem que você aplique uma política de segurança refinada em pontos de controle de rede em toda a sua organização. Serviços da AWS ajudam você a inspecionar e filtrar o tráfego para ajudar a evitar o acesso não autorizado a recursos nos limites do host, da rede e do aplicativo.

- AWS Shield— proteja seus aplicativos da web que são executados AWS com a proteção DDo S gerenciada.
- AWS WAF— proteja seus aplicativos da Web contra explorações comuns da Web e garanta a disponibilidade e a segurança.
- AWS Firewall Manager— configure e gerencie AWS WAF regras Contas da AWS e aplicativos em um local central.
- AWS Systems Manager— Configure e gerencie o Amazon EC2 e sistemas locais para aplicar patches de sistema operacional, criar imagens seguras do sistema e configurar sistemas operacionais seguros.
- Amazon VPC — Provisione uma seção logicamente isolada de AWS onde você pode lançar AWS recursos em uma rede virtual que você define.
- AWS Network Firewall— Implemente proteções de rede essenciais para você VPCs.
- Firewall de DNS do Amazon Route 53 — Proteja suas solicitações de DNS de saída do seu. VPCs
- Acesso Verificado pela AWS— Forneça acesso seguro aos seus aplicativos sem a necessidade de redes privadas virtuais (VPNs).
- Amazon VPC Lattice — Simplifique a service-to-service conectividade, a segurança e o monitoramento.

Detecção de ameaças e monitoramento contínuo — os serviços de AWS monitoramento e detecção fornecem orientação para ajudar a identificar possíveis incidentes de segurança em seu AWS ambiente.

- AWS Security Hub CSPM— Visualize e gerencie alertas de segurança e automatize as verificações de conformidade a partir de um local central.
- AWS Security Hub— Correlacione e enriqueça as descobertas de segurança para priorizar problemas críticos de segurança em suas contas e. Regiões da AWS
- Amazon GuardDuty — Proteja suas cargas Contas da AWS de trabalho com detecção inteligente de ameaças e monitoramento contínuo.
- Amazon Inspector — Automatize as avaliações de segurança para ajudar a melhorar a segurança e a conformidade de seus aplicativos que são implantados em. AWS
- AWS Config— registre e avalie as configurações de seus AWS recursos para permitir a auditoria de conformidade, o rastreamento de alterações de recursos e a análise de segurança.
- Regras do AWS Config— crie regras que atuem automaticamente em resposta às mudanças em seu ambiente, como isolar recursos, enriquecer eventos com dados adicionais ou restaurar a configuração para um estado conhecido como bom.
- AWS Security Incident Response— Automatize a resposta, a investigação e a remediação de incidentes de segurança com playbooks e fluxos de trabalho predefinidos.
- AWS CloudTrail— Acompanhe a atividade do usuário e o uso da API para permitir a governança e a auditoria operacional e de risco do seu Conta da AWS.
- Amazon Detective — Analise e visualize dados de segurança para chegar rapidamente à causa raiz de possíveis problemas de segurança.
- AWS Lambda— Execute código sem provisionar ou gerenciar servidores para que você possa escalar sua resposta programada e automatizada a incidentes.

Conformidade e privacidade de dados — AWS oferece uma visão abrangente do seu status de conformidade e monitora continuamente seu ambiente usando verificações de conformidade automatizadas com base nas AWS melhores práticas e nos padrões do setor que sua empresa segue.

- AWS Artifact— use um portal de autoatendimento gratuito para obter acesso sob demanda a relatórios de AWS segurança e conformidade e selecionar contratos on-line.
- AWS Audit Manager— audite continuamente seu AWS uso para simplificar a forma como você avalia o risco e a conformidade com as regulamentações e os padrões do setor.

Histórico do documento

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

Alteração	Descrição	Data
Reestruturação e atualizações de conteúdo	• Orientações adicionadas para o Security Hub e o AWS Nitro Enclaves. • Reestruturou o AWS SRA para focar na arquitetura principal e transferiu as seções de aprofundamento para guias separados para gerenciamento de identidad e, segurança perimetral, análise forense cibernética, IA generativa e IoT. • A orientação existente foi atualizada para incluir detalhes adicionais sobre AWS CloudTrail AWS Config,, Amazon Detective , AWS Firewall Manager Amazon GuardDuty, IAM Access Analyzer, Amazon Security Lake, e. AWS Shield Advanced AWS Audit Manager	22 de dezembro de 2025
Principais atualizações	• Foram adicionadas informações sobre o novo gerenciamento centraliz	29 de agosto de 2025

ado de acesso do usuário raiz, políticas de controle de recursos (RCPs) e políticas declarativas do IAM.

- Referências atualizadas do CSPM do Security Hub ao novo CSPM do Security Hub.
- Incluiu novos recursos de serviço para Amazon GuardDuty e Security Hub CSPM.
- Orientação AWS Security Incident Response de serviço adicionada.
- Orientações detalhadas atualizadas do IAM para incluir o VPC Lattice para machine-to-machine gerenciamento de identidades.
- Foi adicionada uma nova orientação aprofundada: SRA para IoT.

Adições e esclarecimentos	• Na seção da conta do Security Tooling, atualizei a AWS KMS orientação. • Na seção Gerenciamento de identidade do cliente, expandiu as informações sobre a autorização do API Gateway. • A seção Generative AI foi atualizada para adicionar uma consideração de design para OU e design de conta. • Na seção do repositório de códigos AWS SRA, foram adicionadas informações sobre a nova solução de gerenciamento de patches.	12 de setembro de 2024

Principais atualizações	• Foram adicionadas duas seções para uma orientação arquitetônica aprofundada: IA generativa usando o Amazon Bedrock e gerenciamento de identidade. • As seções Amazon Detective AWS Identity and Access Management Access Analyzer, Amazon Inspector, AWS Artifact, AWS Config, Amazon Security Lake AWS Security Hub CSPMe_CloudFrontAmazon foram atualizadas com novos recursos de serviço. • A seção do repositório de códigos AWS SRA foi atualizada para incluir a nova opção de implantação do Terraform e a adição das soluções AWS Shield Advanced AMI Bakery.	7 de junho de 2024

Principais atualizações	• As seções Conta de rede e Conta de aplicativo foram atualizadas para adicionar diretrizes arquitetônicas para Amazon Verified Permissions e Amazon VPC Lattice. Acesso Verificado pela AWS • Foi adicionada uma orientação arquitetônica aprofundada com base na funcionalidade de segurança. • Foram adicionadas novas orientações sobre como Serviços da AWS usar AI/ML para fornecer melhores resultados de segurança. • Foram adicionadas orientações sobre como planejar sua arquitetura de segurança em fases.	4 de novembro de 2023
Adição do Security Lake	As seções da conta do Security Tooling e da conta do Log Archive foram atualizadas para adicionar orientações de design relacionadas ao Amazon Security Lake.	22 de setembro de 2023

Atualizações menores	• A orientação existente foi atualizada para refletir os novos Serviços da AWS recursos e as melhores práticas. • Orientação arquitetônica atualizada para AWS CloudTrail, Centro de Identidade do AWS IAM, e segurança de ponta.	10 de maio de 2023
Pesquisa	Foi adicionada uma pequena pesquisa para entender melhor como você usa o AWS SRA em sua organização.	14 de dezembro de 2022
Arquivos de origem para diagramas de arquitetura de referência	Na seção Arquitetura de referência de AWS segurança , foi adicionado um arquivo de download que fornece os diagramas de arquitetura deste guia em formato editável PowerPoint .	17 de novembro de 2022
Atualizações na seção Fundamentos de segurança	Na seção Fundamentos de segurança, atualizei as informações sobre os pilares do Well-Architected Framework e os princípios de design de segurança.	27 de setembro de 2022

Principais adições e atualizações	• Foram adicionadas informações sobre como usar o AWS SRA e as principais diretrizes de implementação. • Foram adicionadas orientações arquitetônicas para outros AWS Artifact, Serviços da AWS como Amazon Inspector, AWS RAM Amazon Route 53,,,, AWS Control Tower AWS Audit Manager Directory Service, Amazon Cognito e Network Access Analyzer. • A orientação existente foi atualizada para refletir os novos AWS service (Serviço da AWS) recursos e as melhores práticas.	25 de julho de 2022
—	Publicação inicial	23 de junho de 2021

AWS Glossário de orientação prescritiva

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

Números

7 Rs

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

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

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

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

A

ABAC

Consulte controle de acesso baseado em atributo.

serviços abstraídos

Veja serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

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

migração ativa-passiva

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

AGGREGATE FUNCTION

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

AI

Veja inteligência artificial.

AIOps

Veja operações de inteligência artificial.

anonimização

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

antipadrões

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

controle de aplicações

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

portfólio de aplicações

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

inteligência artificial (IA)

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

operações de inteligência artificial (AIOps)

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

criptografia assimétrica

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

atomicidade, consistência, isolamento, durabilidade (ACID)

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

controle de acesso por atributo (ABAC)

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

fonte de dados autorizada

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

Zona de disponibilidade

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

AWS Estrutura de adoção da nuvem (AWS CAF)

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

para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

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

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot malicioso

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

BCP

Veja planejamento de continuidade de negócios

gráfico de comportamento

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

sistema big-endian

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

classificação binária

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

filtro de bloom

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

blue/green deployment (implantação azul/verde)

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

bot

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

botnet

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

ramo

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

Acesso de emergência

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

estratégia brownfield

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

cache do buffer

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

capacidade de negócios

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

planejamento de continuidade de negócios (BCP)

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

C

CAF

Veja AWS Cloud Adoption Framework.

implantação canário

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

CCoE

Veja Centro de Excelência da Nuvem.

CDC

Veja captura de dados de alteração.

captura de dados de alterações (CDC)

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

engenharia do caos

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

CI/CD

Veja integração e entrega contínuas.

classificação

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

criptografia no lado do cliente

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

Centro de excelência em nuvem (CCoE)

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

computação em nuvem

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

modelo operacional em nuvem

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

estágios de adoção da nuvem

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

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

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

CMDB

Veja banco de dados de gerenciamento de configuração.

repositório de código

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

cache frio

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

dados frios

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

visão computacional (CV)

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

desvio de configuração

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

banco de dados de gerenciamento de configuração (CMDB)

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

pacote de conformidade

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

integração contínua e entrega contínua (CI/CD)

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

CV

Veja visão computacional.

D

dados em repouso

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

classificação de dados

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

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

desvio de dados

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

dados em trânsito

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

data mesh

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

minimização de dados

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

perímetro de dados

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

pré-processamento de dados

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

proveniência dos dados

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

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

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

linguagem de definição de dados (DDL)

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

linguagem de manipulação de dados (DML)

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

DDL

Veja linguagem de definição de banco de dados.

deep ensemble

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

Aprendizado profundo

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

defense-in-depth

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

administrador delegado

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

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

implantação

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

ambiente de desenvolvimento

Veja ambiente.

controle detectivo

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

mapeamento do fluxo de valor de desenvolvimento (DVSM)

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

gêmeo digital

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

tabela de dimensões

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

desastre

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

Recuperação de desastres (RD)

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

DML

Veja linguagem de manipulação de banco de dados.

design orientado por domínio

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

DR

Veja recuperação de desastres.

Detecção da oscilação

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

DVSM

Veja mapeamento do fluxo de valor de desenvolvimento.

E

EDA

Veja análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

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

intercâmbio eletrônico de dados (EDI)

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

criptografia

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

chave de criptografia

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

endianismo

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

endpoint

Veja endpoint de serviço.

serviço de endpoint

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

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

planejamento de recursos empresariais (ERP)

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

criptografia envelopada

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

ambiente

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

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

epic

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

ERP

Veja planejamento de recursos empresariais.

análise exploratória de dados (EDA)

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

F

tabela de fatos

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

Antecipar-se à falha

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

delimitação de isolamento contra falhas

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

ramificação de recursos

Veja ramificação.

recursos

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

importância do recurso

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

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

transformação de recursos

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

prompt few shot

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

FGAC

Veja controle de acesso refinado.

Controle de acesso refinado (FGAC)

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

migração flash-cut

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

FM

Veja modelo de base.

modelo de base (FM)

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

G

IA generativa

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

bloqueio geográfico

Veja restrições geográficas.

restrições geográficas (bloqueio geográfico)

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

Fluxo de trabalho do GitFlow

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

golden image

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

estratégia greenfield

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

barreira de proteção

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

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

H

HA

Veja alta disponibilidade.

migração heterogênea de bancos de dados

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

alta disponibilidade (HA)

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

modernização de historiador

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

dados de hold-out

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

migração homogênea de bancos de dados

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

dados quentes

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

hotfix

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

período de hipercuidados

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

eu

IaC

Veja infraestrutura como código.

Política baseada em identidade

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

aplicação ociosa

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

IIoT

Veja Internet das Coisas Industrial.

infraestrutura imutável

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

VPC de entrada (admissão)

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

migração incremental

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

Indústria 4.0

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

infraestrutura

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

Infraestrutura como código (IaC)

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

Internet industrial das coisas (IIoT)

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

VPC de inspeção

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

Internet das coisas (IoT)

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

interpretabilidade

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

IoT

Veja Internet das Coisas.

Biblioteca de informações de TI (ITIL)

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

Gerenciamento de serviços de TI (ITSM)

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

ITIL

Veja biblioteca de informações de TI.

ITSM

Veja gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

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

zona de pouso

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

grande modelo de linguagem (LLM)

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

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em rótulo.

privilégio mínimo

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

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

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

LLM

Veja grande modelo de linguagem.

ambientes inferiores

Veja ambiente.

M

machine learning (ML)

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

ramificação principal

Veja ramificação.

Malware

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

Serviços gerenciados

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

sistema de execução de manufatura (MES)

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

MAP

Veja Programa de Aceleração da Migração.

mecanismo

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

conta de membro

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

MES

Veja sistema de execução de manufatura.

Transporte de Telemetria de Enfileiramento de Mensagens (MQTT)

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

microsserviço

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

arquitetura de microsserviços

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

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

Programa de Aceleração da Migração (MAP)

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

migração em escala

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

fábrica de migração

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

metadados de migração

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

padrão de migração

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

Avaliação de Portfólio para Migração (MPA)

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

Avaliação de Preparação para Migração (MRA)

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

estratégia de migração

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

ML

Veja machine learning.

modernização

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

avaliação de preparação para modernização

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

aplicações monolíticas (monólitos)

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

MPA

Veja Avaliação do Portfólio para Migração.

MQTT

Veja Transporte de Telemetria de Enfileiramento de Mensagens.

classificação multiclasse

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

infraestrutura mutável

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

O

OAC

Veja controle de acesso de origem.

OAI

Veja identidade de acesso de origem.

OCM

Veja gerenciamento de alterações organizacionais.

migração offline

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

OI

Veja integração de operações.

Ola

Veja acordo de nível operacional.

migração online

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

OPC-UA

Veja Open Process Communications - Unified Architecture.

Open Process Communications - Unified Architecture (OPC-UA)

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

acordo de nível operacional (OLA)

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

análise de prontidão operacional (ORR)

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

tecnologia operacional (TO)

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

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

integração de operações (OI)

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

trilha organizacional

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

gerenciamento de alterações organizacionais (OCM)

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

controle de acesso de origem (OAC)

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

Identidade do acesso de origem (OAI)

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

ORR

Veja análise de prontidão operacional.

OT

Veja tecnologia operacional.

VPC de saída (egresso)

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

P

limite de permissões

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

Informações de identificação pessoal (PII)

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

PII

Veja informações de identificação pessoal.

manual

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

PLC

Veja controlador lógico programável.

PLM

Veja gerenciamento do ciclo de vida do produto.

política

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

persistência poliglota

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

avaliação do portfólio

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

predicado

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

pushdown de predicados

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

controle preventivo

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

principal (entidade principal)

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

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

Privacidade por design

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

zonas hospedadas privadas

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

controle proativo

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

gerenciamento do ciclo de vida do produto (PLM)

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

ambiente de produção

Veja ambiente.

controlador lógico programável (PLC)

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

encadeamento de prompts

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

pseudonimização

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

publish/subscribe (pub/sub)

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

Q

plano de consulta

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

regressão de planos de consultas

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

R

Matriz RACI

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

RAG

Veja geração aumentada via recuperação.

ransomware

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

Matriz RASCI

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

RCAC

Veja controle de acesso por linha e coluna.

réplica de leitura

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

Redefinir arquitetura

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

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

objetivo de tempo de recuperação (RTO)

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

refatorar

Veja 7 Rs.

Região

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

regressão

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

redefinir a hospedagem

Veja 7 Rs.

versão

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

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

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

política baseada em recurso

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

matriz responsável, accountable, consultada, informada (RACI)

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

controle responsivo

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

reter

Veja 7 Rs.

Retirada

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

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

alternância

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

controle de acesso por linha e coluna (RCAC)

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

RPO

Veja objetivo de ponto de recuperação.

RTO

Veja objetivo de tempo de recuperação.

runbook

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

S

SAML 2.0

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

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

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja política de controle de serviço.

secret

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

segurança desde a concepção

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

controle de segurança

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

hardening da segurança

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

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

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

automação de resposta de segurança

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

Criptografia do lado do servidor

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

política de controle de serviços (SCP)

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

service endpoint (endpoint de serviço)

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

acordo de serviço (SLA)

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

indicador de nível de serviço (SLI)

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

objetivo de nível de serviço (SLO)

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

modelo de responsabilidade compartilhada

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

SIEM

Veja sistema de gerenciamento de eventos e informações de segurança.

ponto único de falha (SPOF)

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

SLA

Veja cacordo de serviço.

SLI

Veja indicador de nível de serviço.

SLO

Veja objetivo de nível de serviço.

split-and-seed modelo

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

SPOF

Veja ponto único de falha.

esquema em estrela

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

padrão strangler fig

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

sub-rede

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

controle supervisório e aquisição de dados (SCADA)

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

symmetric encryption (criptografia simétrica)

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

testes sintéticos

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

prompt do sistema

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

T

tags

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

variável-alvo

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

lista de tarefas

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

ambiente de teste

Veja ambiente.

treinamento

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

gateway de trânsito

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

fluxo de trabalho baseado em troncos

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

Acesso confiável

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

tuning (ajustar)

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

equipe de duas pizzas

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

U

incerteza

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

tarefas indiferenciadas

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

ambientes superiores

Veja ambiente.

V

aspiração

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

controle de versões

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

emparelhamento da VPC

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

Vulnerabilidade

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

W

cache quente

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

dados mornos

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

função de janela

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

workload

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

workstreams

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

WORM

Veja gravação única e várias leituras.

WQF

Veja AWS Workload Qualification Framework.

gravação única e várias leituras (WORM)

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

Z

exploração de dia zero

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

vulnerabilidade de dia zero

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

prompt zero shot

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

aplicação zumbi

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

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