AWSOrientação prescritiva

AWSArquitetura de referência de segurança

AWSOrientação prescritiva: AWSArquitetura de referência de segurança

Table of Contents

AWSArquitetura de referência de segurança (AWSSRA)

Amazon Web Services (AWS)

Dezembro de 2022 (histórico do documento (p. 73))

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

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

A arquitetura e as recomendações anexas são baseadas em nossas experiências coletivas com clientes corporativos da AWS. Este documento é uma referência — um conjunto abrangente de diretrizes para usar os serviços da AWS para proteger um ambiente específico — e os padrões de solução no repositório de código do AWS SRA (p. 68) foram projetados para a arquitetura específica ilustrada nesta referência. Cada cliente terá requisitos diferentes. Como resultado, o design do seu ambiente da AWS 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 vivo de diretrizes e é atualizado periodicamente com base em novos serviços e lançamentos de recursos, feedback de clientes e no cenário de ameaças em constante mudança. Cada atualização incluirá a data da revisão e o registro de alterações (p. 73) associado.

Embora confiemos em um diagrama de uma página como base, a arquitetura é mais profunda do que um único diagrama de bloco 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 final (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 para suas necessidades.

Este documento está dividido em seis seções e um apêndice:

- O valor do AWS SRA (p. 3) 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 analisam (p. 7) o AWS Cloud Adoption Framework (AWS CAF), o AWS Well-Architected Framework e o AWS Shared Responsibility Model e destacam elementos que são especialmente relevantes para o AWS SRA.
- Organizations, accounts e IAM guardrails (p. 10) da AWS apresentam o serviço AWS Organizations, discutem os recursos e as barreiras de segurança fundamentais e fornecem uma visão geral da nossa estratégia recomendada para várias contas.

- A Arquitetura de Referência de Segurança da AWS (p. 24) é um diagrama de arquitetura de página única que mostra as contas funcionais da AWS e os serviços e recursos de segurança que geralmente estão disponíveis.
- Os recursos do IAM (p. 65) apresentam um resumo e um conjunto de indicadores para a orientação do AWS Identity and Access Management (IAM) que são importantes para sua arquitetura de segurança.
- O repositório de código para exemplos de SRA da AWS (p. 68) fornece uma visão geral do GitHubrepositório associado que contém exemplos de CloudFormation modelos e códigos da AWS para implantar alguns dos padrões discutidos no AWS SRA.

O apêndice (p. 71) contém uma lista dos serviços individuais de segurança, identidade e conformidade da AWS e fornece links para mais informações sobre cada serviço. A seção Histórico do documento (p. 73) fornece um registro de alterações para rastrear versões desse documento. Você também pode assinar um feed RSS para receber notificações de alterações.

> **Note**
>
> Para personalizar os diagramas de arquitetura de referência neste guia com base nas necessidades da sua empresa, você pode baixar o arquivo .zip a seguir e extrair seu conteúdo.
>
> Baixe o arquivo de origem do diagrama (PowerPoint formato Microsoft)

O valor do AWS SRA

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

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

1. Os clientes querem mais informações e padrões recomendados sobre como implantar, configurar e operar os serviços de segurança da AWS de forma holística. Em quais contas e para quais objetivos de segurança os serviços devem ser implantados e gerenciados? Existe uma conta de segurança em que todos ou a maioria dos serviços devem operar? Como a escolha do local (unidade organizacional ou conta da AWS) informa os objetivos de segurança? Quais compensações (considerações de design) devem os clientes conhecer?
2. Os clientes estão interessados em ver diferentes perspectivas para organizar logicamente os diversos serviços de segurança da AWS. 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 guia agrupa os serviços com base nas camadas de proteção alinhadas à estrutura recomendada do seu ambiente da AWS.
3. Os clientes estão procurando orientação e exemplos para integrar os serviços de segurança da maneira mais eficaz. Por exemplo, qual é a melhor forma de alinhar e conectar o AWS Config a outros serviços para fazer o trabalho pesado em pipelines automatizados de auditoria e monitoramento? Os clientes estão pedindo orientação sobre como cada serviço de segurança da AWS depende ou dá suporte a outros serviços de segurança.

Abordamos cada uma delas no AWS SRA. A primeira prioridade na lista (para onde as coisas vão) é o foco do diagrama de arquitetura principal e das discussões que o acompanham neste documento. Fornecemos uma arquitetura recomendada do AWS Organizations e uma account-by-account descrição de quais serviços vão para onde. Para começar com a segunda prioridade na lista (como pensar no conjunto completo de serviços de segurança), leia a seção Aplicar serviços de segurança em toda a sua organização da AWS (p. 17). Esta seção descreve uma maneira de agrupar serviços de segurança de acordo com a estrutura dos elementos em sua organização da AWS. Além disso, essas mesmas ideias se refletem na discussão da conta do aplicativo (p. 56), 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 conta mais ampla. Por fim, a terceira prioridade (integração de serviços) se reflete em toda a orientação, especialmente na discussão de serviços individuais nas seções detalhadas da conta desta documentação e no código no repositório de códigos do AWS SRA.

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 dos ativos do AWS SRA (diagrama de arquitetura, orientação escrita e exemplos de código).

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

Se você está apenas começando sua jornada na nuvem da AWS — configurando seu primeiro conjunto de contas — ou planejando aprimorar um ambiente estabelecido da AWS, 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 seu conjunto específico de tecnologias, habilidades, objetivos de segurança e requisitos de conformidade. Se você sabe que vai criar e lançar mais cargas de trabalho, você pode usar sua versão personalizada do AWS SRA e usá-la como base para a arquitetura de referência de segurança da sua organização.

- Analise (e revise) os designs e os recursos que você já implementou.

Se você já tem um projeto e uma implementação de segurança, vale a pena comparar o que você tem com o AWS SRA. O AWS SRA foi projetado para ser abrangente e fornece 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 os serviços da AWS. Se seus projetos de segurança divergirem ou até mesmo discordarem das diretrizes 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 de SRA da AWS. Talvez seus requisitos específicos de conformidade, regulamentação ou segurança organizacional exijam configurações de serviço específicas. Ou, em vez de usar os serviços da AWS, você pode ter uma preferência de recurso para um produto da Rede de Parceiros da AWS ou 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 antigas, recursos da AWS ou restrições comerciais que não se aplicam mais. Essa é uma boa oportunidade para analisar, priorizar todas as atualizações e adicioná-las ao local apropriado de sua lista de pendências de engenharia. O que quer que você descubra ao avaliar sua arquitetura de segurança à luz do AWS SRA, você achará importante documentar essa análise. Ter esse registro histórico de decisões e suas justificativas pode ajudar a informar e priorizar decisões future.

- 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 do repositório de código (p. 68) e no GitHub repositório público. Eles não apenas permitem que os engenheiros desenvolvam exemplos de alta qualidade dos padrões na orientação do AWS SRA, mas também incorporam controles de segurança recomendados, como políticas de senha do AWS Identity and Access Management (IAM), acesso público à conta de bloqueio do Amazon Simple Storage Service (Amazon S3) e Amazon EC2 criptografia padrão do Amazon Elastic Block Store (Amazon EBS) e integração com a AWS Control Tower para que os controles sejam aplicados ou removidos à medida que novas contas da AWS são integradas ou desativadas.

- Saiba mais sobre os serviços e recursos de segurança da AWS.

As orientações e discussões no AWS SRA incluem recursos importantes, bem como considerações de implantação e gerenciamento para serviços individuais relacionados à segurança e à segurança da AWS. Um recurso do AWS SRA é que ele fornece uma introdução de alto nível sobre a amplitude dos serviços de segurança da AWS e como eles funcionam juntos em um ambiente com várias contas. Isso complementa o aprofundamento dos recursos e da configuração de cada serviço encontrado em outras fontes. Um exemplo disso é a discussão (p. 33) de como o AWS Security Hub ingere descobertas de segurança de uma variedade de serviços da AWS, produtos de parceiros da AWS 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 vinculada 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 do AWS Key Management Service (AWS KMS) e em quais contas essas chaves serão gerenciadas. Entender as características de sua organização — as várias equipes e responsabilidades — ajudará você a adaptar o AWS SRA para melhor atender às suas necessidades. 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. A AWS recomenda um processo de tomada de decisão descentralizado em que as equipes de carga de trabalho são 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 do AWS SRA

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

- AWS Organizations e uma estratégia apropriada para várias contas são elementos necessários de sua arquitetura de segurança. A separação adequada de cargas de trabalho, equipes e funções fornece as bases para a separação de tarefas e defense-in-depth estratégias. O guia aborda isso mais detalhadamente em uma seção posterior (p. 14).
- Defense-in-depth é uma importante consideração de design para selecionar controles de segurança para sua organização. Ele ajuda você a injetar os controles de segurança apropriados em diferentes camadas da estrutura do AWS Organizations, o que ajuda a minimizar o impacto de um problema: se houver um problema com uma camada, existem controles que isolam outros recursos valiosos de TI. O AWS SRA demonstra como os diferentes serviços da AWS funcionam em diferentes camadas do conjunto de tecnologias da AWS e como o uso desses serviços em combinação ajuda você a alcançar o sucesso defense-in-depth. Esse defense-in-depth conceito na AWS será discutido mais detalhadamente em uma seção posterior (p. 17), com exemplos de design mostrados em Conta do aplicativo (p. 56).
- Use a grande variedade de componentes de segurança em vários serviços e recursos da AWS para criar uma infraestrutura de nuvem robusta e resiliente. Ao adaptar o AWS SRA às suas necessidades específicas, considere não apenas a função principal dos serviços e recursos da AWS (por exemplo, autenticação, criptografia, monitoramento, política de permissão), mas também como eles se encaixam na estrutura de sua arquitetura. Uma seção posterior (p. 19) do guia descreve como alguns serviços operam em toda a sua organização da AWS. Outros serviços funcionam melhor em uma única conta, e alguns são projetados para conceder ou negar permissão a diretores individuais. Considerar essas duas perspectivas ajuda você a criar uma abordagem de segurança em camadas mais flexível.
- Sempre que possível (conforme detalhado nas seções posteriores), use os serviços da AWS que podem ser implantados em todas as contas (distribuídos em vez de centralizados) e crie um conjunto consistente de barreiras compartilhadas que podem ajudar a proteger suas cargas de trabalho contra o uso indevido e ajudar a reduzir o impacto dos eventos de segurança. O AWS SRA usa o AWS Security Hub (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 (serviço de registro), atividade da API em seu ambiente) e Amazon Macie (classificação de dados) como um conjunto básico de serviços da AWS a serem implantados em todas as contas da AWS.

- Use o recurso de administração delegada do AWS Organizations, onde ele é suportado, conforme explicado posteriormente na seção de administração delegada (p. 33) do guia. Isso permite que você registre uma conta de membro da AWS como administrador dos serviços suportados. A administração delegada oferece flexibilidade para que diferentes equipes de sua empresa usem contas separadas, conforme apropriado para suas responsabilidades, para gerenciar os serviços da AWS em todo o ambiente. Além disso, usar um administrador delegado ajuda você a limitar o acesso e gerenciar a sobrecarga de permissões da conta de gerenciamento do AWS Organizations.
- Implemente monitoramento, gerenciamento e governança centralizados em suas organizações da AWS. Ao usar serviços da AWS que oferecem suporte à agregação de várias contas (e às vezes em várias regiões), juntamente com recursos de administração delegada, você capacita suas equipes centrais de segurança, rede e engenharia de 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 a AWS Control Tower para configurar e governar seu ambiente AWS de várias contas com a implementação de controles de segurança pré-criados para inicializar sua construção de arquitetura de referência de segurança. A 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 Control Tower (cFCT) para basear as contas gerenciadas pela AWS Control Tower com controles de segurança, configurações de serviços e governança adicionais, conforme demonstrado pelo repositório de código SRA da AWS. O recurso de fábrica de contas provisiona automaticamente novas contas com modelos configuráveis com base na configuração de conta aprovada para padronizar contas em suas AWS Organizations. Você também pode estender a governança para uma conta individual existente da AWS inscrevendo-a em uma unidade organizacional (OU) que já é governada pela AWS Control Tower.
- Os exemplos de código do AWS SRA demonstram como você pode automatizar a implementação de padrões dentro do guia do AWS SRA usando a infraestrutura como código (IaC). A codificação dos padrões oferece a capacidade de tratar o IaC de forma semelhante a outros aplicativos em sua organização, nos quais os testes podem ser automatizados antes que as implantações sejam concluídas. O IaC também ajuda a garantir a consistência e a repetibilidade com a implantação de grades de proteção em vários ambientes (por exemplo, SDLC ou específicos da região). Os exemplos de código da SRA usam a AWS Control Tower com personalizações para a AWS Control Tower (cFCT) para acelerar a incorporação do IaC em um ambiente da AWS.

Fundamentos de segurança

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

A arquitetura de referência de segurança da AWS se alinha a três bases de segurança da AWS: o AWS Cloud Adoption Framework (AWS CAF), o AWS Well-Architected e o modelo de responsabilidade compartilhada da AWS.

A AWS 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 sua empresa e em todo o ciclo de vida de TI. O AWS CAF organiza a orientação em seis áreas de foco, chamadas de perspectivas. Cada perspectiva abrange responsabilidades distintas de propriedade ou gerenciadas por partes interessadas funcionalmente relacionadas. Em geral, as perspectivas de negócios, pessoas e governança se concentram nas capacidades dos negócios; enquanto as perspectivas de plataforma, segurança e operações se concentram nas capacidades técnicas.

- A perspectiva de segurança do AWS CAF ajuda você a estruturar a seleção e a implementação de controles em sua empresa. Seguir as recomendações atuais da AWS no pilar de segurança pode ajudá-lo a atender aos seus requisitos comerciais e regulatórios.

O AWS Well-Architected ajuda 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 clientes e parceiros da AWS avaliarem arquiteturas e implementarem projetos que podem ser escalados ao longo do tempo. Acreditamos que ter cargas de trabalho bem arquitetadas aumenta muito a probabilidade de sucesso nos negócios.

- O pilar de segurança Well-Architected 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 seus requisitos comerciais e regulatórios seguindo as recomendações atuais da AWS. 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 a AWS e o cliente. Esse modelo compartilhado pode ajudar a aliviar sua carga operacional à medida que a AWS opera, gerencia e controla os componentes do sistema operacional e da camada de virtualização do host 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 fornecido pela AWS. Para Serviços abstratos, como o Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB, a 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 de gerenciamento de identidade e acesso (IAM) da AWS para aplicar as permissões apropriadas. Esse modelo compartilhado geralmente é descrito dizendo que a AWS é responsável pela segurança da nuvem (ou seja, por proteger a infraestrutura que executa todos os serviços oferecidos na nuvem da AWS) e que você é responsável pela segurança na nuvem (conforme determinado pela nuvem da AWS). serviços que você seleciona).

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

Recursos de segurança

A perspectiva de segurança do AWS CAF descreve nove recursos que ajudam você a obter a confidencialidade, a integridade e a 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 ambiente da AWS de 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, remediar e mitigar continuamente as vulnerabilidades de segurança.
- Proteção da 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 com eficácia aos incidentes de segurança.

Princípios Princípios princípios

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 da Well-Architected descrevem o que você pode começar a fazer. Eles são refletidos de forma muito deliberada neste SRA da AWS e consistem no seguinte:

- Implemente uma base de identidade sólida — implemente o princípio do menor privilégio e imponha a separação de tarefas com a autorização apropriada para cada interação com seus recursos da AWS. Centralize o gerenciamento de identidades e busque eliminar a dependência de credenciais estáticas de longo prazo.
- Habilite a rastreabilidade — monitore, gere alertas e audite ações e mudanças em seu ambiente em tempo real. Integre a coleta de registros e métricas com sistemas para investigar e agir 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 baseados em software melhoram sua capacidade de escalar com segurança de forma mais rápida e econômica. Crie arquiteturas seguras e implemente controles que são 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 manualmente os dados. Isso reduz o risco de manuseio incorreto ou modificação e erro humano ao lidar com dados confidenciais.
- Prepare-se para eventos de segurança — Prepare-se para um incidente com políticas e processos de gerenciamento e investigação de incidentes alinhados aos seus requisitos organizacionais. Execute simulações de resposta a incidentes e use ferramentas com automação para aumentar sua velocidade de detecção, investigação e recuperação.

Componentes básicos da SRA — organizações, contas e grades de proteção da AWS

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

Os serviços de segurança da AWS, seus controles e interações são melhor empregados com base na estratégia de várias contas da AWS e nas barreiras de gerenciamento de identidade e acesso. Essas barreiras definem a capacidade de implementação de privilégios mínimos, separação de funções 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 no AWS SRA.

Uma conta da AWS fornece limites de segurança, acesso e cobrança para seus recursos da AWS e permite que você obtenha independência e isolamento de recursos. O uso de várias contas da AWS desempenha um papel importante na forma como você atende aos seus requisitos de segurança, conforme discutido na seção Benefícios do uso de várias contas da AWS do whitepaper Organizando seu ambiente da AWS 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 estabeleça 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 o AWS Organizations, é usada para isolar ambientes de produção dos ambientes de desenvolvimento e teste ou para fornecer um forte limite lógico entre cargas de trabalho que processam dados de diferentes classificações, como o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) ou a Lei de Portabilidade e Responsabilidade de Seguros de Health (HIPAA). Embora você possa começar sua jornada na AWS com uma única conta, a 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 recursos da AWS. As permissões são concedidas a entidades do IAM conhecidas como diretores (usuários, grupos e funções). Por padrão, os diretores começam sem permissões. As entidades do IAM não podem fazer nada na AWS até que você lhes conceda permissões, e você pode configurar barreiras que se apliquem de forma tão ampla quanto toda a sua organização da AWS ou tão refinadas quanto uma combinação individual de princípio, ação, recurso e condições.

Usando o AWS Organizations para fins de segurança

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

AWS Organizations Access ajuda você a gerenciar e governar centralmente seu ambiente à medida que você expande e escala seus recursos da AWS Ao usar o AWS Organizations, você pode criar programaticamente novas contas da AWS, alocar recursos, agrupar contas para organizar suas cargas de trabalho e aplicar políticas a contas ou grupos de contas para governança. Uma organização da AWS Account da AWS para que você possa administrá-las como uma só unidade. Ele tem uma conta de gerenciamento e zero ou mais contas de membros. A maioria de suas cargas de trabalho reside em contas de membros, exceto por alguns processos gerenciados centralmente que devem residir na conta de gerenciamento ou em contas designadas como administradores delegados para serviços específicos da AWS. Você pode fornecer ferramentas e acesso de um local central para que sua equipe de segurança gerencie as necessidades de segurança em nome de uma organização da AWS. Você pode reduzir a duplicação de recursos compartilhando recursos essenciais em sua organização da AWS. Você pode agrupar contas em unidades organizacionais (OUs) da AWS, que podem representar diferentes ambientes com base nos requisitos e na finalidade da carga de trabalho.

Com o AWS Organizations, você pode usar políticas de controle de serviços (SCPs) para aplicar barreiras de permissão no nível da organização, UO ou da conta da AWS. Essas barreiras de proteção se aplicam aos diretores da 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 vincula um SCP a uma OU, ele é herdado pelas OUs secundárias e pelas contas da OU. Os SCPs não concedem nenhuma permissão. Em vez disso, os SCPs especificam as permissões máximas para uma organização, UO ou conta da AWS. Você ainda precisa anexar políticas baseadas em identidade ou em recurso para diretores ou recursos em suas contas da AWS Por exemplo, se um SCP negar acesso a todo o Amazon S3, um administrador afetado pelo SCP não terá acesso ao Amazon S3, mesmo que lhe seja explicitamente concedido acesso por meio de uma política do IAM. Para obter informações detalhadas sobre como as políticas do IAM são avaliadas, o papel dos SCPs e como o acesso é finalmente concedido ou negado, consulte a lógica de avaliação de políticas na documentação do IAM.

O AWS Control Tower oferece uma forma simplificada de configurar e controlar várias contas. Ele automatiza a configuração de contas em sua organização da AWS, automatiza o provisionamento, aplica barreiras de proteção (que incluem controles preventivos e de detetive) e fornece um painel para visibilidade. Uma política de gerenciamento do IAM, um limite de permissões, é anexada a entidades do IAM (usuários ou funções) do IAM e define as permissões máximas que uma política baseada em identidade pode conceder a uma entidade do IAM.

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

A configuração padrão do AWS Organizations suporta o uso de 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 conjunto de ações. As declarações de negação exigem menos manutenção do que uma lista de permissões, porque você não precisa atualizá-las quando a AWS adiciona novos serviços. As declarações de negação geralmente têm menos caracteres, então é mais fácil ficar dentro do tamanho máximo para SCPs. Em uma declaração em que o elemento `Effect` tem um valor de `Deny`, você também pode restringir o acesso a recursos específicos ou definir condições para quando as SCPs estão em vigor. Por outro lado, uma instrução Allow 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 usar SCPs na documentação do AWS Organizations.

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 até 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 da conta da AWS até a OU.

- Idealmente, você usaria uma combinação de estratégias de lista de negação e lista de permissão. Use a lista de permissões para definir a lista de serviços permitidos da AWS aprovados para uso em uma organização da AWS e anexe esse SCP à raiz da sua organização da AWS. Se você tiver um conjunto diferente de serviços permitidos por seu ambiente de desenvolvimento, você anexaria os respectivos SCPs em cada UO. Em seguida, você pode usar a lista de negação para definir barreiras corporativas negando explicitamente ações específicas do IAM.

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

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

A conta de gerenciamento (também chamada de conta de gerenciamento da organização da AWS ou conta de gerenciamento da organização) é única e diferenciada de todas as outras contas no AWS Organizations. É a conta que cria a organização da AWS. A partir dessa conta, você pode criar contas da AWS na organização da AWS, convidar outras contas existentes para a organização da AWS (ambos os tipos são considerados contas de membros), remover contas da organização da AWS e aplicar políticas do IAM à raiz, às OUs ou às contas dentro da organização da AWS.

A conta de gerenciamento implanta barreiras de segurança universais por meio de SCPs e implantações de serviços (como a AWS CloudTrail) que afetarão todas as contas dos membros na organização da 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. Não é possível alterar a conta de gerenciamento de uma organização da AWS Uma conta da AWS pode ser membro de apenas uma organização da AWS 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 precisem delas. Dois recursos que ajudam você a fazer isso são acesso confiável e administrador delegado. Você pode usar o acesso confiável para habilitar um serviço da AWS, chamado serviço da AWS, chamado serviço confiável, a executar tarefas em sua organização da AWS Isso requer a concessão de permissões ao serviço confiável, mas não afeta de outra forma as permissões para entidades do IAM. Você pode usar o acesso confiável para especificar configurações e detalhes de configuração que você gostaria que o serviço confiável mantivesse nas contas da sua organização da AWS em seu nome. Por exemplo, a seção de contas de gerenciamento (p. 26) de organizações do AWS SRA explica como conceder ao CloudTrail serviço da AWS acesso confiável para criar uma trilha CloudTrail organizacional em todas as contas da sua organização da AWS.

Alguns serviços da AWS oferecem suporte ao recurso de administrador delegado no AWS Organizations. Com esse recurso, serviços compatíveis podem registrar uma conta da AWS na organização da AWS

Esse recurso oferece flexibilidade para que diferentes equipes da sua empresa usem contas separadas, conforme apropriado para suas responsabilidades, para gerenciar os serviços da AWS em todo o ambiente. Os serviços de segurança da AWS no AWS SRA que atualmente oferecem suporte ao administrador delegado incluem o AWS IAM Identity Center (sucessor do AWS Single Sign-On), AWS Config, AWS Firewall Manager, Amazon GuardDuty, AWS IAM Access Analyzer, Amazon Macie, AWS Security Hub, Amazon Detective, AWS Audit Manager, Amazon Inspector e AWS Systems Manager. O uso do recurso de administrador delegado é enfatizado no AWS SRA como uma prática recomendada, e delegamos a administração de serviços relacionados à segurança na conta do Security Tooling.

Estrutura de contas dedicadas

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

Uma conta da AWS fornece limites de segurança, acesso e cobrança para seus recursos da AWS e permite que você obtenha 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 de OUs fundamentais para essas funções específicas, dividido em OUs de infraestrutura e segurança. Essas recomendações de UO e contas capturam um subconjunto de nossas diretrizes mais amplas e abrangentes para AWS Organizations e design de estruturas de várias contas. Para obter um conjunto completo de recomendações, consulte Organizando seu ambiente da AWS usando várias contas na documentação da AWS 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 na AWS. Essas contas dedicadas ajudam a garantir a separação de tarefas, apoiam 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, estamos focados nas contas de produção (prod) 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 e gerenciamento centrais de todas as regiões e contas da AWS. A conta da AWS que hospeda a raiz da organização da AWS.
Ferramentas de segurança	Segurança	Contas dedicadas da AWS para operar serviços de segurança amplamente aplicáveis (como Amazon GuardDuty, AWS Security Hub, AWS Audit Manager, Amazon Detective, Amazon Inspector e AWS Config), monitorar contas da

		AWS e automatizar alertas e respostas de segurança.
Arquivo de registros	Segurança	Contas dedicadas da AWS para ingestão e arquivamento de todos os registros e backups de todas as regiões e contas da AWS. Isso deve ser projetado como armazenamento imutável.
Rede	Infraestrutura	A porta de entrada 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, da segurança e de outras infraestruturas de aplicativos individuais.
Serviços compartilhados	Infraestrutura	Essa conta oferece suporte aos serviços que vários aplicativos e equipes usam para entregar 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 organização da AWS e executam as cargas de trabalho. (Às vezes, elas 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.

Organização e estrutura de contas da AWS do AWS SRA

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

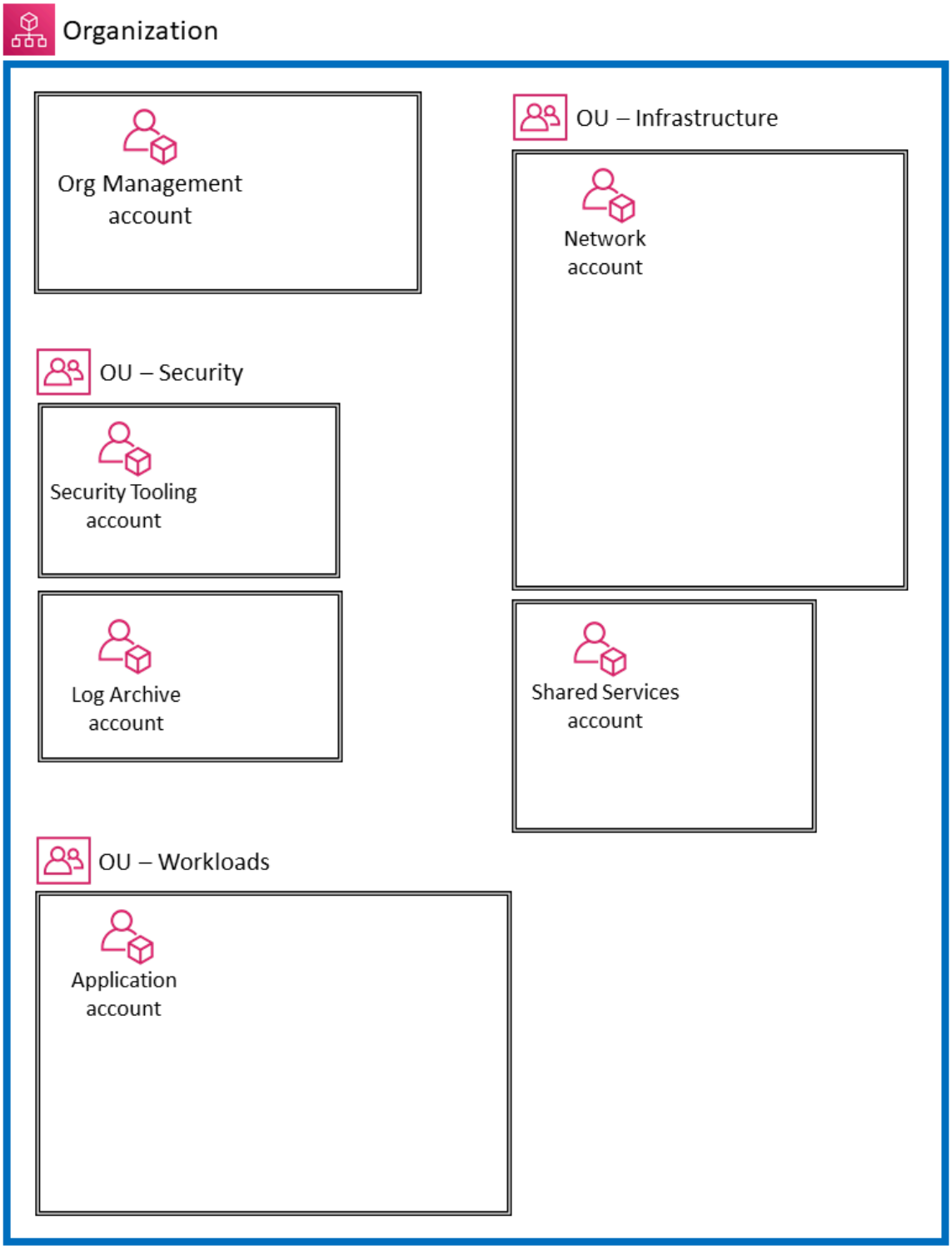
O diagrama a seguir captura a estrutura de alto nível do AWS SRA sem exibir serviços específicos. Ela reflete a estrutura de contas dedicadas discutida na seção anterior, e incluímos o diagrama aqui para orientar a discussão em torno dos principais componentes da arquitetura:

- Todas as contas que são mostradas no diagrama fazem parte de uma única organização da AWS

- No canto superior esquerdo do diagrama está a conta de gerenciamento da organização, que é usada para criar a organização da AWS.
- Abaixo da conta de gerenciamento da organização está a OU de segurança com duas contas específicas: uma para ferramentas de segurança e outra para arquivamento de registros.
- No lado direito está a OU de infraestrutura com a conta de rede e a conta de serviços compartilhados.
- Na parte inferior do diagrama está a OU de cargas de trabalho, que está associada a uma conta de aplicativo que hospeda o aplicativo corporativo.

Para essa discussão, todas as contas são consideradas contas de produção (prod) que operam em uma única região da AWS. Quando um serviço regional, como Amazon S3 GuardDuty, Amazon ou AWS Key Management Service (AWS KMS), é exibido dentro de uma conta, esse serviço é configurado e gerenciado de dentro dessa conta.

Ao hospedar uma organização da AWS com um grande conjunto de contas, é benéfico ter uma camada de orquestração que facilite a implantação e a governança da conta. A AWS Os exemplos de código do AWS SRA no GitHubrepositório demonstram como você pode usar a solução Customizations for AWS Control Tower (cFct) para implantar as estruturas recomendadas pela AWS SRA.

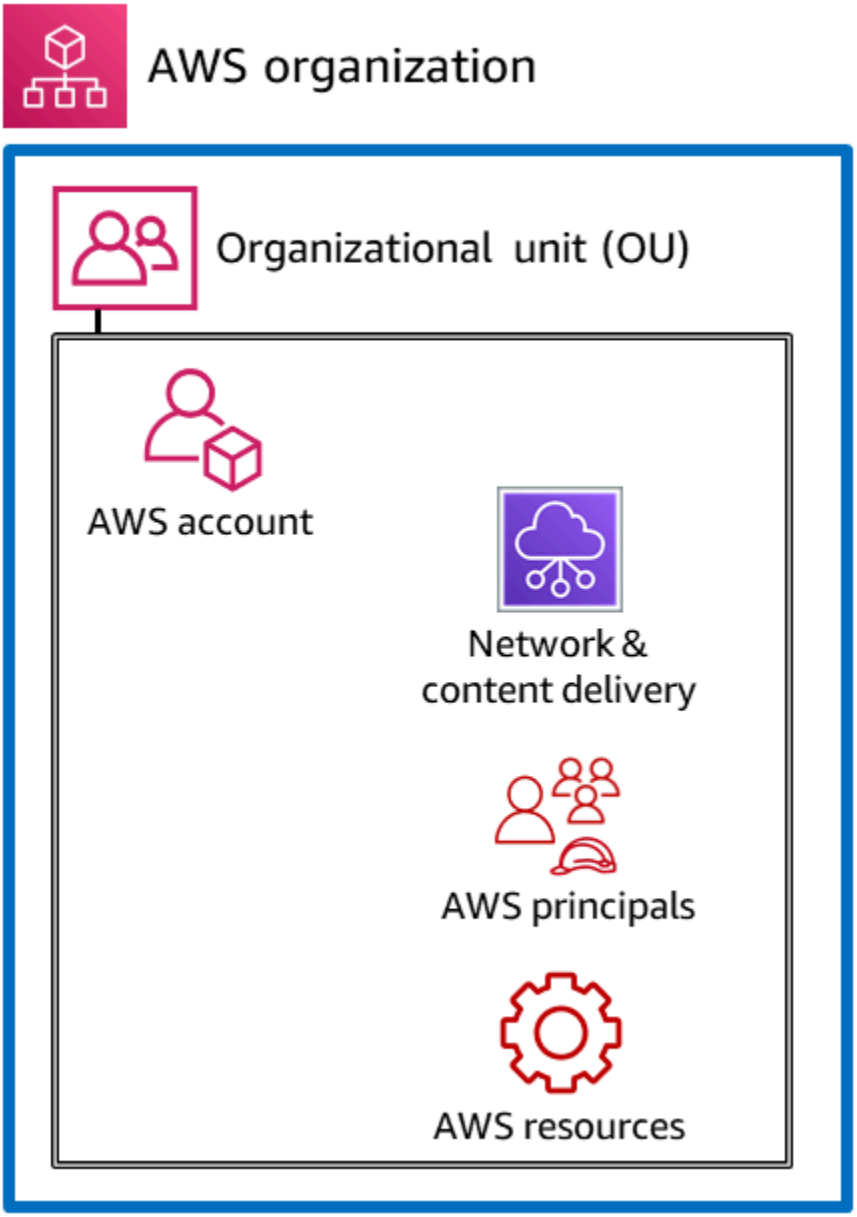

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

Aplique serviços de segurança em toda a sua organização da AWS

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

Conforme descrito em uma seção anterior (p. 3), os clientes estão procurando uma forma adicional de pensar e organizar estrategicamente o conjunto completo de serviços de segurança da AWS. 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. Combinar os serviços da AWS com 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, a Amazon GuardDuty pode ser sua primeira consideração.

Como complemento a essa visão funcional, você também pode visualizar sua segurança com uma visão estrutural transversal. Ou seja, além de perguntar: “Quais serviços da AWS devo usar para controlar e proteger minhas identidades, acesso lógico ou mecanismos de detecção de ameaças?” , você também pode perguntar: “Quais serviços da AWS devo aplicar em toda a minha organização da AWS? Quais são as camadas de defesa que eu deveria implementar para proteger as instâncias do Amazon EC2 no centro do meu aplicativo?” Nessa visualização, você mapeia os serviços e recursos da AWS para camadas em seu ambiente da AWS. Alguns serviços e recursos são ideais para implementar controles em toda a sua organização da AWS. Por exemplo, bloquear o acesso público a buckets do Amazon S3 é um controle específico nessa camada. Isso deve ser feito preferencialmente 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 uma 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 infraestrutura da AWS. O diagrama a seguir mostra seis camadas em um ambiente típico da AWS: organização da AWS, unidade organizacional (OU), conta, infraestrutura de rede, diretores e recursos.



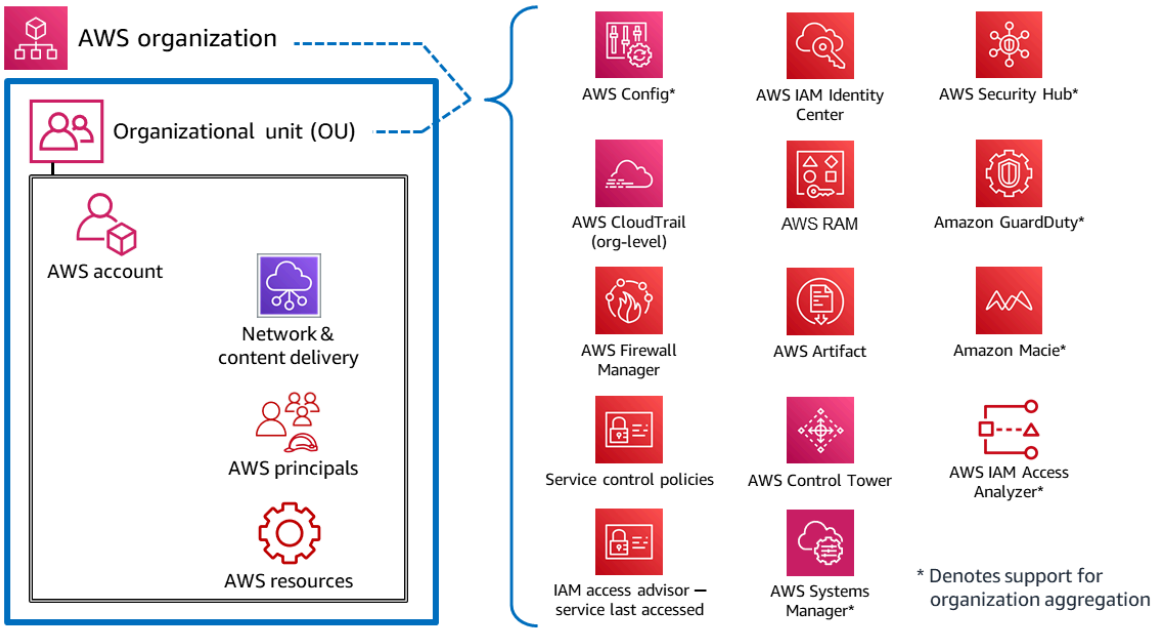
Entender os serviços nesse contexto estrutural, incluindo os controles e proteções em cada camada, ajuda você a planejar e implementar uma defense-in-depth estratégia em seu ambiente da AWS. Com essa perspectiva, você pode responder a perguntas de cima para baixo (por exemplo, “Quais serviços estou usando para implementar controles de segurança em toda a minha organização da AWS?”) e de baixo para cima (por exemplo, “Quais serviços gerenciam controles nessa instância do EC2?”). Nesta seção, examinamos os elementos de um ambiente da AWS 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 ambiente da AWS.

Para maior clareza, fornecemos breves descrições de como alguns dos serviços atendem aos objetivos estabelecidos. A próxima seção (p. 24) fornece uma discussão mais aprofundada sobre os serviços individuais em cada conta da AWS.

Contas em toda a organização ou em várias contas

No nível superior, há serviços e recursos da AWS projetados para aplicar recursos ou barreiras de governança e controle em várias contas em uma organização da AWS (incluindo toda a organização ou OUs específicas). As Políticas de controle de serviço (SCPs) são um bom exemplo de um recurso do IAM que fornece uma proteção preventiva da AWS Outro exemplo é a AWS CloudTrail, que fornece monitoramento por meio de uma trilha organizacional que registra todos os eventos de todas as contas da AWS nessa organização da AWS. Essa trilha abrangente é diferente das trilhas individuais que podem ser criadas em cada conta. Um terceiro exemplo é o AWS Firewall Manager, que você pode usar para configurar, aplicar e gerenciar vários recursos em todas as contas da sua organização da AWS: regras do AWS WAF, regras do AWS WAF Classic, proteções do AWS Shield Advanced, grupos de segurança da Amazon Virtual Private Cloud (Amazon VPC), políticas do AWS Network Firewall e políticas do Amazon Route 53 Resolver DNS Firewall.

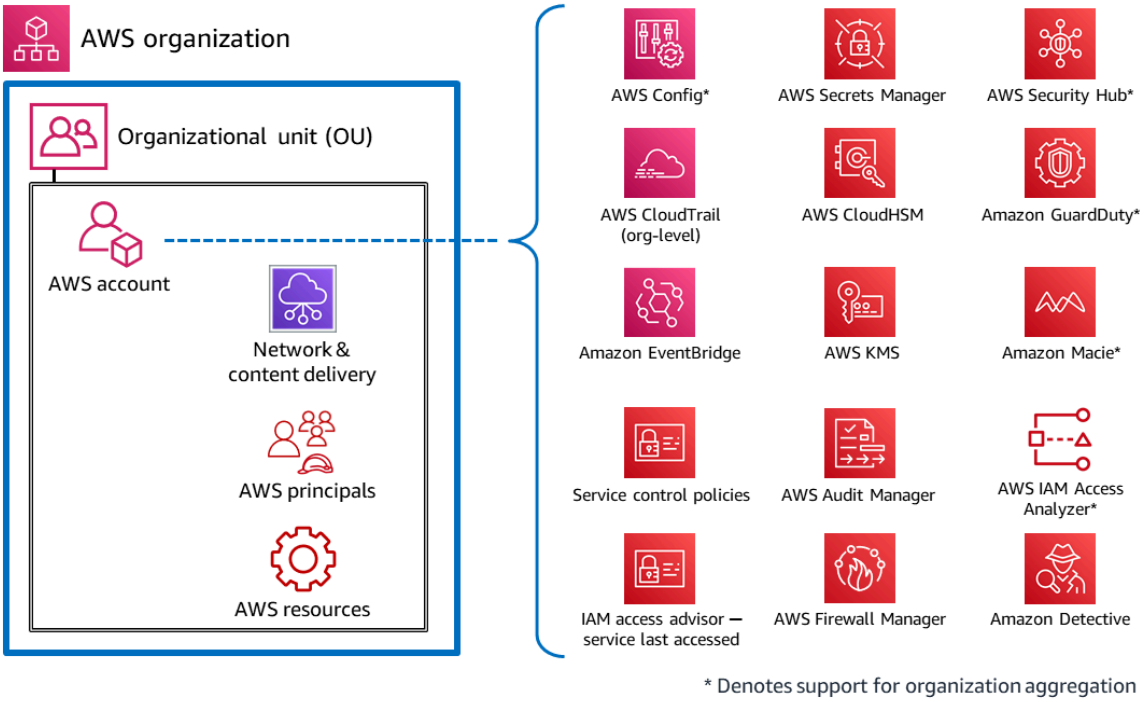
Os serviços marcados com um asterisco* no diagrama a seguir operam com um escopo duplo: em toda a organização e com foco na conta. Esses serviços basicamente monitoram ou ajudam a controlar a segurança em uma conta individual. No entanto, eles também oferecem suporte à capacidade de agregar seus resultados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



Conda AWS

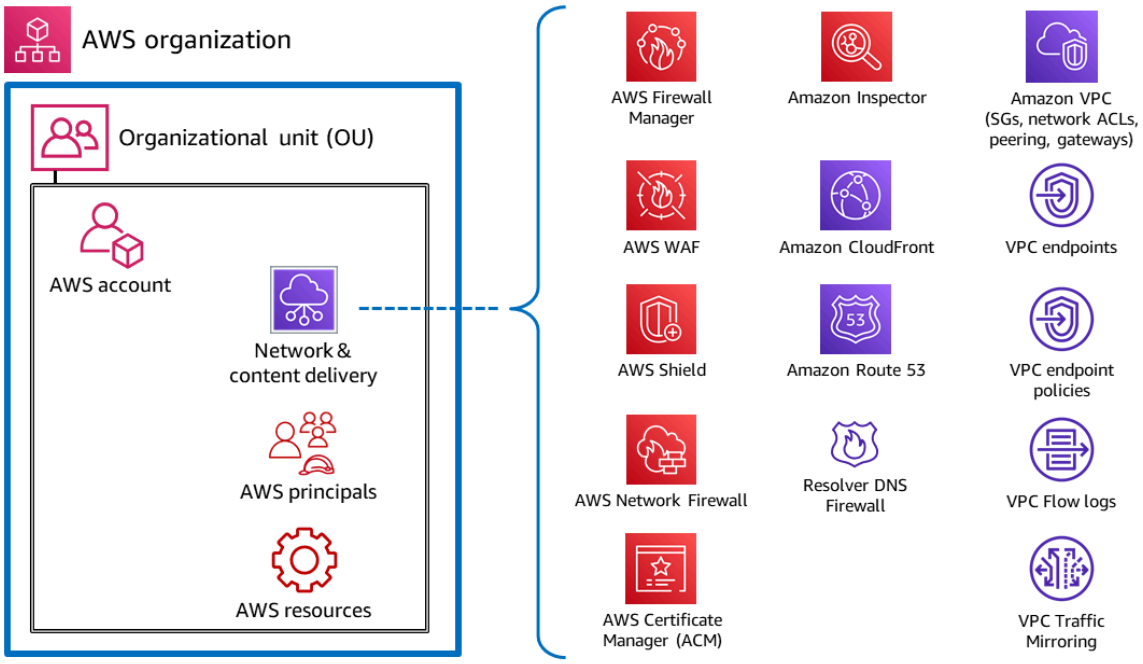
Nas OUs, existem serviços que ajudam a proteger vários tipos de elementos em uma conta da AWS. Por exemplo, o AWS Secrets Manager geralmente é gerenciado a partir de uma conta específica e protege recursos (como credenciais de banco de dados ou informações de autenticação), aplicativos e serviços da AWS nessa conta. O AWS IAM Access Analyzer pode ser configurado para gerar descobertas quando recursos específicos são acessíveis por diretores fora da conta da AWS. Conforme mencionado na seção anterior, muitos desses serviços também podem ser configurados e administrados dentro do AWS Organizations, para que possam ser gerenciados em várias contas. Esses serviços são marcados com

um asterisco (*) no diagrama. Eles também facilitam a agregação de resultados de várias contas e a entrega 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 para equipes de segurança centralizadas. A Amazon GuardDuty é um exemplo desse serviço. GuardDutymonitora recursos e atividades associados a uma única conta, e GuardDuty as descobertas de várias contas de membros (como todas as contas em uma organização da AWS) 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 cargas de trabalho da AWS, há muitos serviços e recursos de segurança da AWS dedicados a esses recursos. Por exemplo, o Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas cargas de trabalho da AWS em busca de vulnerabilidades. Essas verificações incluem verificações de acessibilidade da rede que indicam que há caminhos de rede permitidos para instâncias do Amazon EC2 em seu ambiente. A Amazon Virtual Private Cloud (Amazon VPC) permite definir uma rede virtual na qual você pode executar recursos da AWS Essa rede virtual é muito semelhante a uma rede tradicional e inclui uma variedade de recursos e benefícios. Os VPC endpoints permitem que você conecte de forma privada a VPC aos serviços da AWS compatíveis e aos serviços do VPC endpoint desenvolvidos pela AWS, PrivateLink sem exigir 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

Os diretores da AWS e os recursos da AWS (junto com as políticas do IAM) são os elementos fundamentais no gerenciamento de identidade e acesso na AWS. Um diretor autenticado na AWS pode realizar ações e acessar os recursos da AWS. Uma entidade de segurança pode ser autenticada como um usuário raiz da AWS, ou um usuário do IAM, ou assumindo uma função.

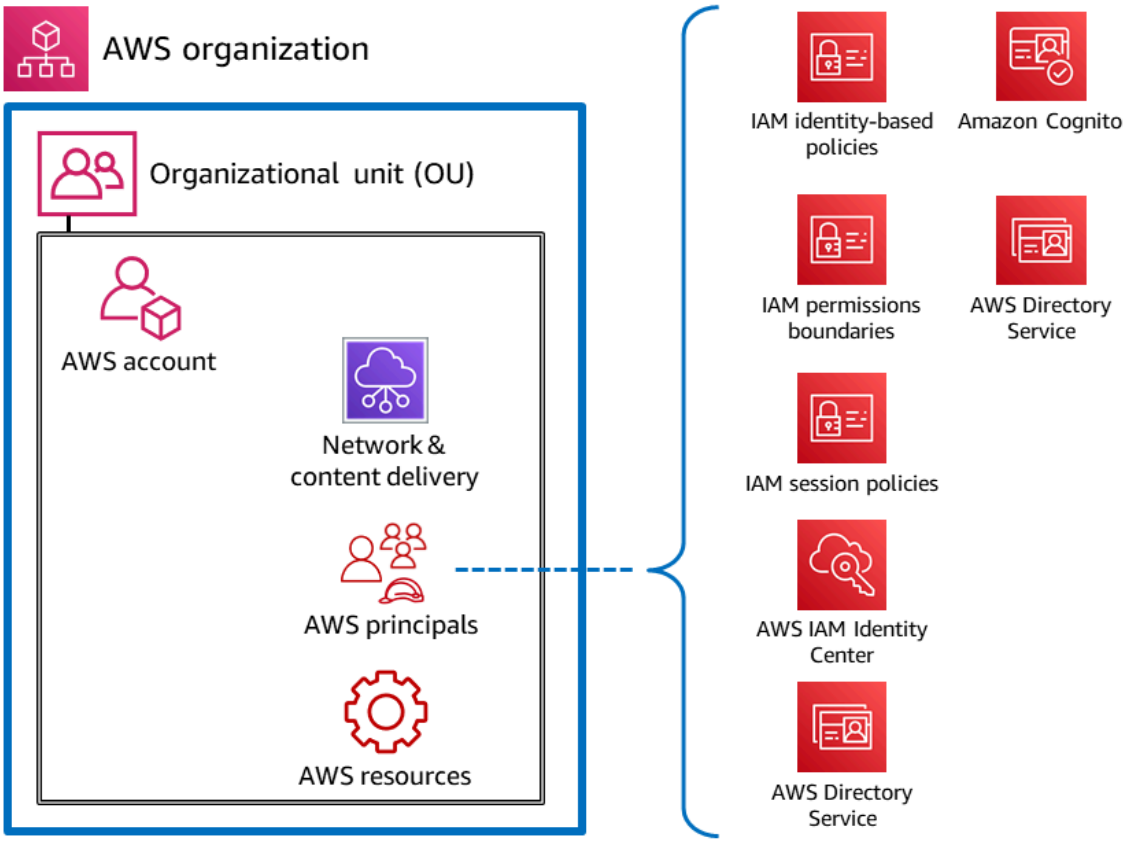
> Note
>
> Não crie chaves de API persistentes associadas ao usuário raiz da AWS. O acesso ao usuário raiz deve ser limitado somente às tarefas que exigem um usuário raiz e somente por meio de um rigoroso processo de exceção. Para obter as melhores práticas para proteger o usuário raiz da sua conta da AWS

Um recurso da AWS Access é um objeto que existe dentro de um serviço da AWS Os exemplos incluem uma instância do AWS, um tópico do CloudFormation AWS, um tópico do Amazon Simple Notification Service (Amazon SNS) e um bucket do AWS As Políticas do IAM são objetos que definem permissões quando são associadas a uma identidade do IAM (usuário, grupo ou função) ou recurso da AWS As Políticas baseadas em identidade são documentos de política que você anexa a a a um diretor (funções, usuários e grupos de usuários) para controlar quais ações um diretor pode realizar, em quais recursos e em que condições. As Políticas baseadas em recurso são documentos de política que você anexa a a a um recurso, como um bucket do S3. Essas políticas concedem permissão para a entidade principal especificada executar ações específicas nesse recurso e definem as condições para essa permissão. As políticas baseadas em recursos são políticas em linha. A seção de recursos do IAM (p. 65) se aprofunda nos tipos de políticas do IAM e como elas são usadas.

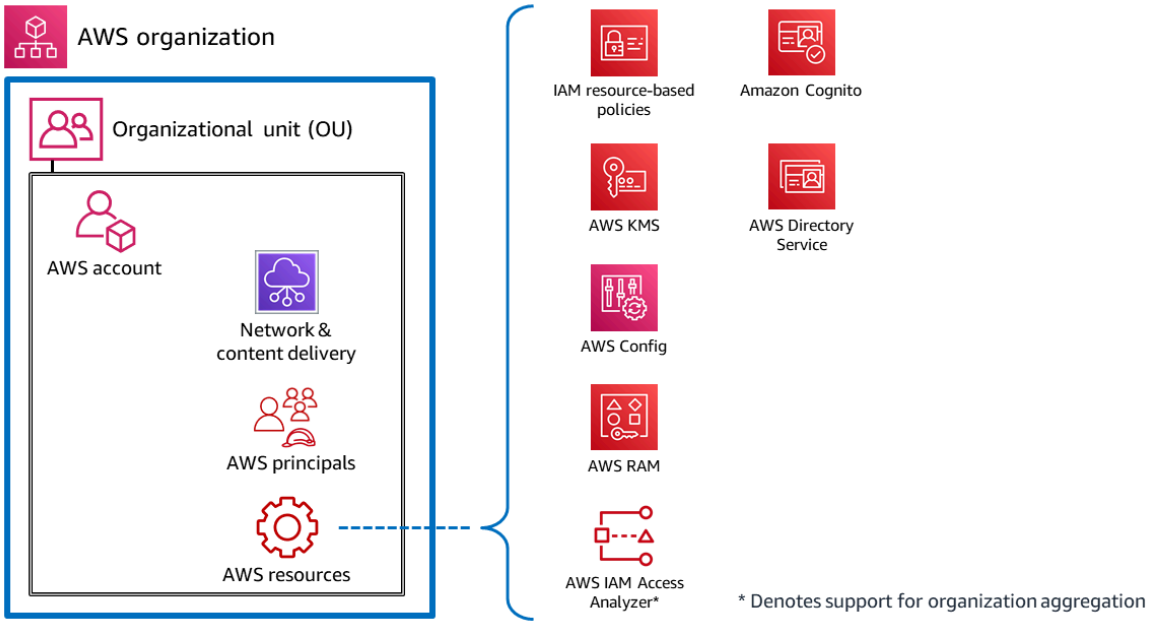
Para simplificar as coisas nesta discussão, listamos os serviços e recursos de segurança da AWS para entidades do IAM que têm como objetivo principal operar ou se inscrever em diretores de contas. Mantemos essa simplicidade e, ao mesmo tempo, reconhecemos a flexibilidade e a amplitude dos efeitos das políticas de permissão do IAM. Uma única declaração em uma política pode ter efeitos em vários tipos de entidades da AWS. Por exemplo, embora uma política baseada em identidade do IAM esteja associada a uma entidade do IAM e defina permissões (permitir, negar) para essa entidade, 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 segurança da AWS para diretores da AWS. As Políticas baseadas em identidade são anexadas a objetos de recurso do IAM que são usados para identificação e agrupamento, como usuários, grupos e funções. 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 na AWS. Isso permite que seus administradores reduzam o número de funções que precisam criar, pois vários usuários podem assumir a mesma função, mas ter permissões de sessão exclusivas. O serviço IAM Identity Center é integrado às operações da AWS Organizations e da API da AWS e ajuda você a gerenciar o acesso por SSO e as permissões de usuário em suas contas da AWS no 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 recurso a buckets S3, filas do Amazon Simple Queue Service (Amazon SQS), endpoints do VPC e chaves de criptografia do AWS KMS. É possível usar políticas baseadas em recurso para especificar quem tem acesso ao recurso e quais ações essas pessoas podem realizar nele. As Políticas de bucket do AWS KMS e políticas de VPC endpoint do AWS são tipos de políticas baseadas em recurso. O AWS 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. O AWS Config permite avaliar, auditar e verificar as configurações dos recursos da AWS O AWS Config monitora e registra continuamente as configurações de recursos da AWS e avalia automaticamente as configurações registradas 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 de referência de segurança da AWS

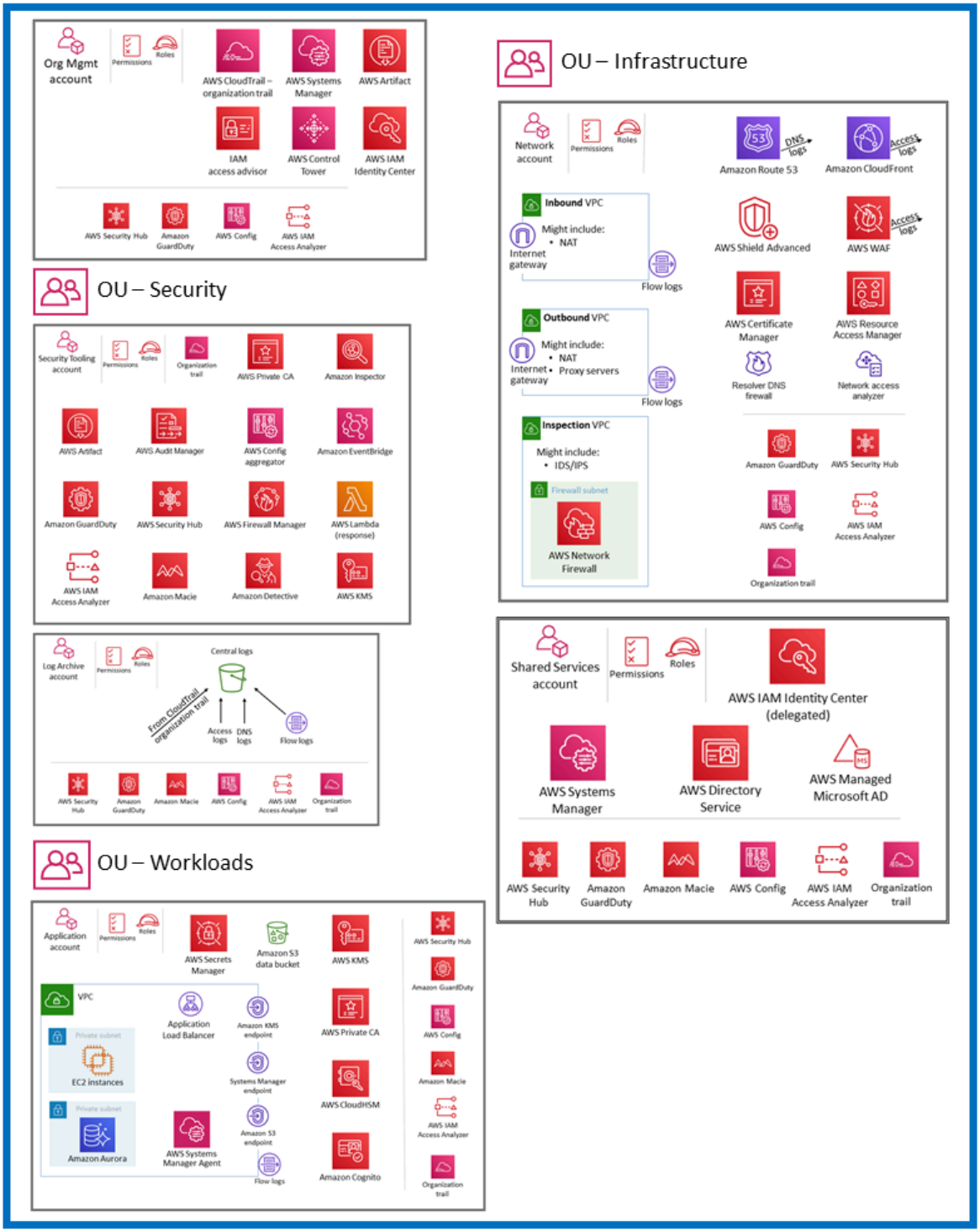
Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra o AWS SRA. Esse diagrama arquitetônico reúne todos os serviços relacionados à segurança da AWS. 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: receber entradas do usuário, fazer alguns cálculos e gerar 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.

Observações

Para simplificar, o diagrama a seguir mostra a arquitetura em um nível intencionalmente alto e obscurece os detalhes de cada conta. Para ver os diagramas de contas individuais com mais detalhes, consulte as seções separadas para OUs e contas.
Para personalizar os diagramas de arquitetura de referência neste guia com base nas necessidades da sua empresa, você pode baixar o arquivo .zip a seguir e extrair seu conteúdo.

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



Para essa arquitetura de referência, o aplicativo web real e a camada de dados são deliberadamente representados da forma mais simples possível, por meio de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) 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 nos níveis 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 relacionados à segurança da AWS disponíveis no momento da publicação. (Consulte o histórico do documento (p. 73).) 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 apropriadas para suas necessidades de infraestrutura, carga de trabalho e segurança, com base no risco.

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

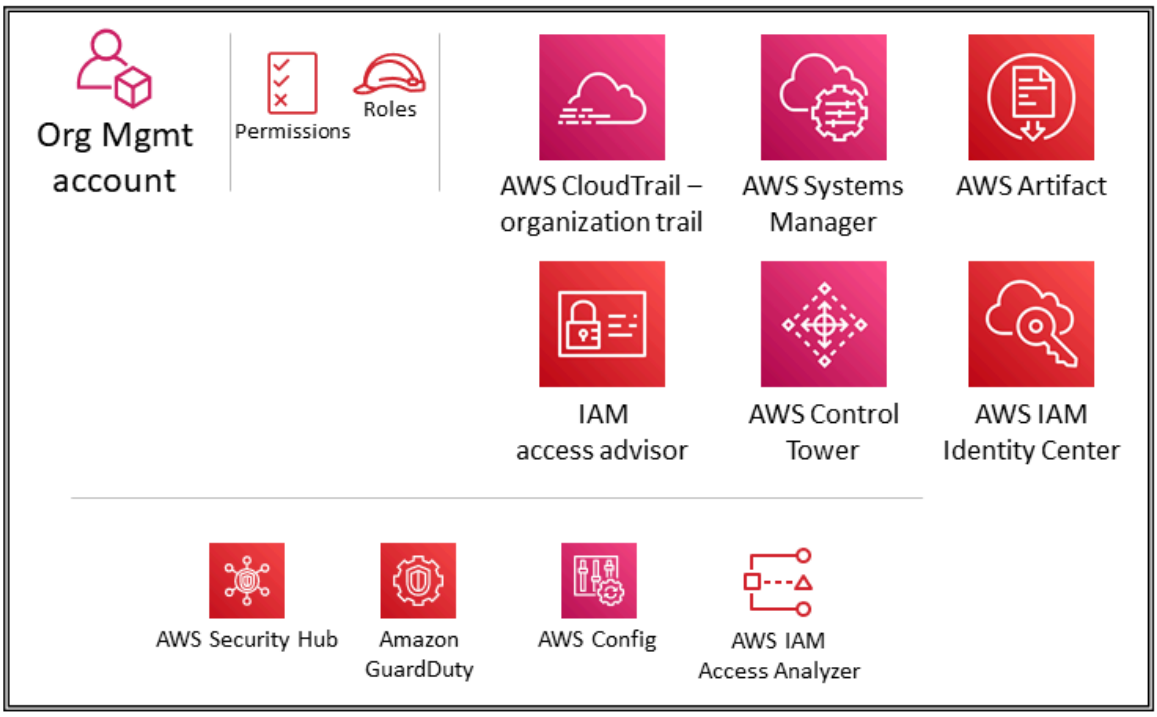
- Breve visão geral do elemento e sua finalidade de segurança no AWS SRA. Para obter descrições mais detalhadas e informações técnicas sobre serviços individuais, consulte o apêndice (p. 71).
- Posicionamento recomendado para habilitar e gerenciar o serviço com mais eficiência. Isso é capturado nos diagramas 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 sobre design. Primeiro, o documento destaca recursos ou configurações opcionais que têm implicações de segurança importantes. Em segundo lugar, 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.

UOs e contas

Conta de gerenciamento da organização

> Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

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



As seções Usando AWS Organizations para fins de segurança (p. 10) e A conta de gerenciamento, acesso confiável e administradores delegados, apresentadas (p. 12) 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 organizacional. 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 caso a AWS precise 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 da organização. 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 o 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 várias contas da AWS que são membros de uma organização. Os SCPs permitem que você defina quais APIs de serviço da AWS podem e não podem ser executadas por entidades do AWS Identity and Access Management (IAM) (como usuários e funções do IAM) nas contas da AWS membros da sua organização. Os SCPs são criados e aplicados a partir da conta de gerenciamento da organização, que é a conta da AWS que você usou ao criar sua organização. Leia mais sobre SCPs na seção Usando AWS Organizations para segurança (p. 10), anteriormente nesta referência.

Se você usar a AWS Control Tower para gerenciar sua organização da AWS, ela implantará um conjunto de SCPs como barreiras 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. Esses SCPs usam automaticamente uma aws-control-tower tag que tem um valor de managed-by-control-tower.

Consideração de design

- Os SCPs afetam somente as contas dos membros na organização da AWS. Embora sejam aplicados a partir da conta de gerenciamento da organização, eles não têm efeito sobre os usuários ou funções nessa conta. Para saber como a lógica de avaliação do SCP funciona e ver exemplos de estruturas recomendadas, consulte a postagem do blog da AWS Como usar políticas de controle de serviços nas AWS Organizations.

AWS CloudTrail

CloudTrail A AWS é um serviço que oferece suporte à governança, conformidade, auditoria operacional e auditoria de risco da sua conta da AWS. Com CloudTrail, você pode registrar, monitorar e reter continuamente as atividades da conta relacionadas às ações em sua infraestrutura da AWS. CloudTrail está integrado com o AWS Organizations, e essa integração pode ser usada para criar uma trilha única que registre em log todos os eventos de todas as contas na organização da AWS. Elas são chamadas de trilhas da organização. Quando você criar uma trilha da organização, será criada uma trilha com o nome especificado em cada conta da AWS da pertencente à sua organização da AWS. A trilha registra a atividade de todas as contas na organização da AWS e os armazena em um único bucket do S3. Todas as contas na organização da AWS podem ver a trilha da organização em sua lista de trilhas, mas as contas da AWS têm acesso limitado a essa trilha. Além disso, por padrão, somente a conta de gerenciamento da organização tem acesso ao bucket do S3. Para obter mais informações sobre essas proteções, consulte a seção Amazon S3 como armazenamento central de registros (p. 45). Para obter mais práticas recomendadas de segurança, consulte a CloudTrail documentação da AWS.

No AWS SRA, CloudTrail aparece na conta de gerenciamento da organização, porque você pode criar uma trilha organizacional somente de dentro da conta de gerenciamento e com as permissões apropriadas do IAM. O bucket S3 da trilha organizacional correspondente para armazenar todos os registros é criado na conta do Log Archive.

Consideração de design

- Se as contas dos membros precisarem usar CloudTrail as informações de uma forma que não seja permitida pela trilha da organização, os gerentes de cada conta da AWS poderão criar uma trilha local com os controles apropriados.

IAM Identity Center

O Centro de Identidade do AWS IAM (sucessor do AWS Single Sign-On) é um serviço de federação de identidade que ajuda você a gerenciar de forma centralizada o acesso por SSO a todas as suas contas, funções e cargas de trabalho na nuvem. O IAM Identity Center também ajuda você a gerenciar o acesso e as permissões a 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 fornecimento em massa pode ser feito usando o System for Cross-Domain Identity Management (SCIM). O IAM Identity Center inclui um portal de usuário no qual seus usuários finais podem encontrar e acessar suas contas, funções, aplicativos em nuvem e aplicativos personalizados atribuídos à AWS em um só lugar.

O IAM Identity Center se integra nativamente com o 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, o gerenciamento do IAM Identity Center pode ser delegado 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 do IAM Identity Center, analise essas considerações. Você encontrará mais informações sobre delegação na seção Conta do Shared Services (p. 53). 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 que são provisionados na conta de gerenciamento da organização.

No console do IAM Identity Center, as contas são exibidas por sua OU encapsulada. Isso permite que você descubra rapidamente suas 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 em que informações específicas do usuário devem ser armazenadas. No entanto, o IAM Identity Center não precisa ser a fonte oficial de informações sobre a força de trabalho, embora possa. 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 em grupo 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 com o repositório de identidades.
- Microsoft Active Directory (AD) — Escolha essa opção se quiser gerenciar usuários em seu próprio Active Directory local ou baseado na nuvem, ou se quiser migrar ou usar o AWS Managed Microsoft AD no AWS Directory Service.
- IdP externo — Escolha essa opção se você preferir gerenciar usuários em um IdP externo de terceiros.

Você pode confiar em um IdP existente que já existe em sua empresa. Isso facilita o gerenciamento do acesso em vários aplicativos e serviços, porque você está criando, gerenciando e revogando o acesso a partir de um único local. Por exemplo, se alguém deixar sua equipe, você poderá revogar seu acesso a todos os aplicativos e serviços (incluindo 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).

Consideração de design

- Use um IdP externo se essa opção estiver disponível para sua empresa. Aproveite o recurso SCIM no IAM Identity Center para automatizar o provisionamento de usuários, grupos e permissões (sincronização). Isso permite que o acesso à AWS permaneça sincronizado com seu fluxo de trabalho corporativo para novos contratados, funcionários que estão migrando para outra equipe e funcionários que estão deixando a empresa.

integridade do IAM

O consultor de acesso do IAM fornece dados de rastreabilidade na forma de informações do último acesso do serviço para suas contas e OUs da AWS. Use esse controle de detetive para contribuir com uma estratégia de privilégio mínimo. Para entidades do IAM, você pode visualizar dois tipos de informações do último acesso: informações de serviço da AWS e informações de ação. 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, UO, conta de membro ou política do IAM em sua organização da AWS. Essas informações estão disponíveis no console do IAM na conta de gerenciamento e também podem ser obtidas programaticamente usando APIs do consultor de acesso do IAM na AWS Command Line Interface (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 últimas informações acessadas 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 às AWS Organizations e operam a partir da conta de gerenciamento da organização.

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

O Explorer é um painel de operações personalizável que fornece informações sobre os recursos da AWS. O Explorer exibe uma visão agregada dos dados operacionais de suas contas da AWS e em todas as regiões da AWS. Isso inclui dados sobre suas instâncias do EC2 e detalhes de conformidade do patch. Depois de concluir a configuração integrada (que também inclui o Systems Manager OpsCenter) dentro do AWS Organizations, você pode agregar dados no Explorer por UO ou para uma organização inteira da AWS. O Systems Manager agrega os dados na conta do AWS Org Management do antes de exibi-los em Explorer.

A seção Workloads UO (p. 56), mais adiante neste guia, discute o uso do Systems Manager Agent (SSM Agent) nas instâncias do EC2 na conta do aplicativo.

AWS Control Tower

O AWS Control Tower fornece uma maneira simples de configurar e controlar um ambiente da AWS com várias contas, chamado de zona de aterrissagem. A AWS Control Tower cria sua landing zone usando o AWS Organizations e fornece gerenciamento e governança contínuos de contas, bem como as melhores práticas de implementação. Você pode usar a 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 ambiente da AWS Control Tower.

O AWS Control Tower tem um conjunto amplo e flexível de recursos. Um recurso importante é sua capacidade de orquestrar os recursos de vários outros serviços da AWS, incluindo o AWS Organizations, o AWS Service Catalog e o IAM Identity Center, para criar uma landing zone. Por exemplo, por padrão, a AWS Control Tower usa CloudFormation a AWS para estabelecer uma linha de base, as políticas de controle de serviços (SCPs) da AWS Organizations para evitar alterações na configuração e as regras do AWS Config para detectar continuamente a não conformidade. A AWS Control Tower emprega planos que ajudam você a alinhar rapidamente seu ambiente de várias contas da AWS com os princípios de design da base de segurança do AWS Well Architected. Entre os recursos de governança, o AWS Control Tower oferece barreiras que impedem a implantação de recursos que não estão em conformidade com as políticas selecionadas.

Você pode começar a implementar a orientação de SRA da AWS com a AWS Control Tower. Por exemplo, a AWS Control Tower estabelece uma organização da AWS com a arquitetura recomendada para várias contas. Ele fornece planos para fornecer gerenciamento de identidades, 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, a AWS Control Tower está dentro da conta de gerenciamento da organização porque a AWS Control Tower usa essa conta para configurar uma organização da AWS automaticamente e designa essa conta como a conta de gerenciamento. Essa conta é usada para faturamento em toda a sua organização da AWS. Também é usado para provisionamento de contas do Account Factory, para gerenciar OUs e gerenciar grades de proteção. Se você estiver lançando o AWS Control Tower em uma organização existente da AWS, poderá usar a conta de gerenciamento existente. A AWS Control Tower usará essa conta como a conta de gerenciamento designada.

Consideração de design

- Se você quiser fazer uma definição de base adicional de controles e configurações em suas contas, você pode usar Customizations for AWS Control Tower (cFCT). Com o cFct, você pode personalizar sua landing zone da AWS Control Tower usando um CloudFormation modelo da AWS e políticas de controle de serviços (SCPs). Você pode implantar o modelo e as políticas personalizados em contas individuais e OUs em sua organização. O cFct se integra aos eventos do ciclo de vida da AWS Control Tower para garantir que as implantações de recursos permaneçam sincronizadas com sua landing zone.

AWS Artifact

O AWS Artifact fornece acesso sob demanda aos relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. Os relatórios disponíveis no AWS Artifact incluem relatórios de controles de sistema e organização (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 da AWS. O AWS Artifact ajuda você a realizar sua devida diligência na AWS com maior transparência em nosso ambiente de controle de segurança. Ele também permite que você monitore continuamente a segurança e a conformidade da AWS com acesso imediato a novos relatórios.

Os contratos da AWS Artifact permitem que você analise, aceite e acompanhe o status dos contratos da AWS, como o Business Associate Addendum (BAA) para uma conta individual e para as contas que fazem parte da sua organização no AWS Organizations.

Você pode fornecer os artefatos de auditoria da AWS aos seus auditores ou reguladores como evidência dos controles de segurança da AWS. Você também pode usar a orientação de responsabilidade fornecida por alguns dos artefatos de auditoria da AWS 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.

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

Consideração de design

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

Guardrails de serviços de segurança distribuídos e centralizados

No AWS SRA, o AWS Security Hub, o Amazon GuardDuty, o AWS Config, o IAM Access Analyzer, as trilhas CloudTrail organizacionais da AWS e, muitas vezes, o Amazon Macie são implantados com administração delegada apropriada ou agregação à conta do Security Tooling. Isso permite um conjunto consistente de barreiras de proteção em todas as contas e também fornece monitoramento, gerenciamento e governança centralizados em toda a sua organização da AWS. Você encontrará esse grupo de serviços em cada tipo de conta representada no AWS SRA. Eles devem fazer parte dos serviços da AWS que devem ser provisionados como parte do processo de integração e definição de base de sua conta. O

repositório deGitHub código fornece um exemplo de implementação de serviços focados na segurança da AWS em suas contas, incluindo a conta do AWS Org Management.

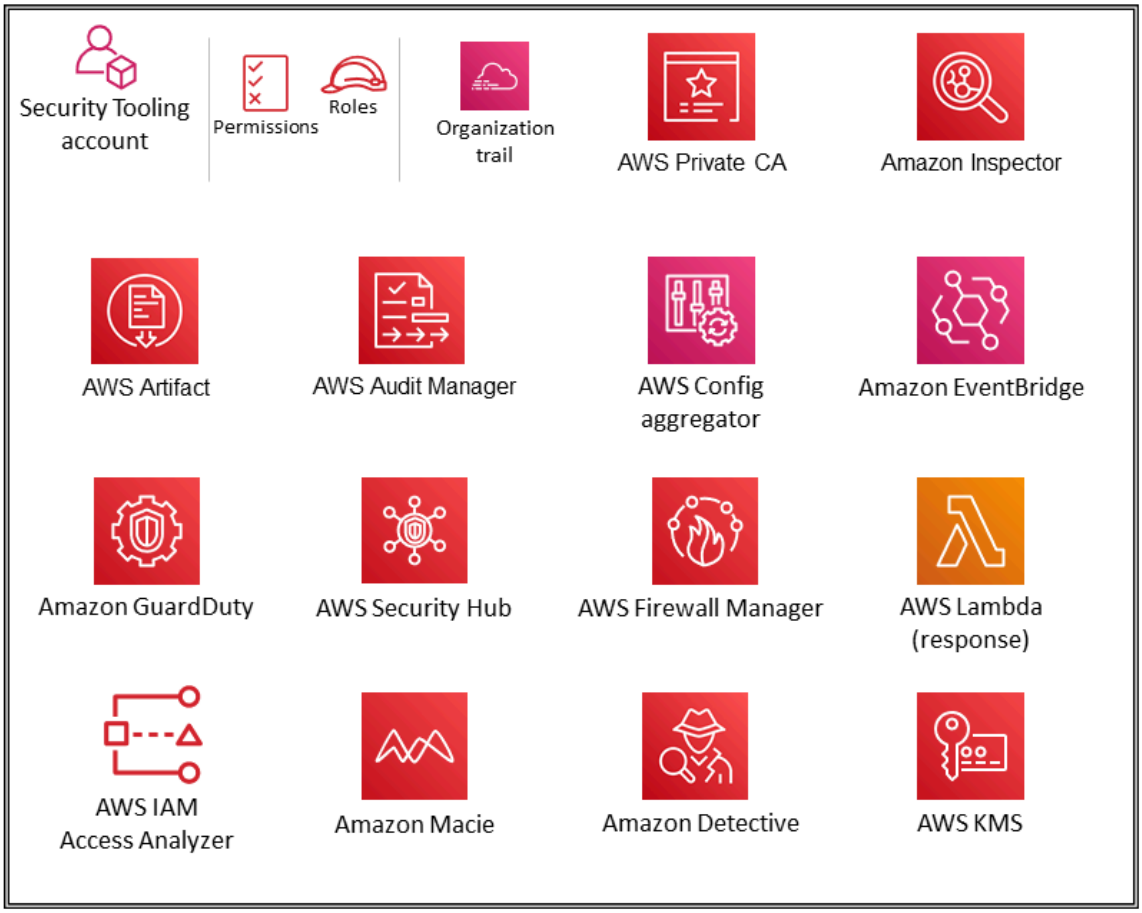
Além desses serviços, o AWS SRA inclui dois serviços focados em segurança, o AWS Detective e o AWS Audit Manager, que oferecem suporte à integração e à funcionalidade de administrador delegado nas AWS Organizations. No entanto, eles não estão incluídos como parte dos serviços recomendados para definição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

- Você tem uma equipe dedicada ou um grupo de recursos que executam essas funções de análise forense digital e auditoria de TI. O AWS Detective é melhor utilizado pelas equipes de analistas de segurança, e o AWS 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, no início do seu projeto e, em seguida, desenvolvê-las usando serviços que fornecem recursos adicionais.

Security OU - Conta de ferramentas de segurança

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

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



A conta Security Tooling é dedicada a operar serviços de segurança, monitorar contas da AWS 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, ao monitoramento e à resposta.
- Mantenha a infraestrutura de segurança centralizada apropriada para monitorar os dados das operações de segurança e manter a rastreabilidade. A detecção, a investigação e a 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 de uma defense-in-depth 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 de somente leitura/auditoria para visualizar informações de toda a organização da AWS são típicas, enquanto as funções de gravação/modificação são limitadas em número, rigorosamente controladas, monitoradas e registradas.

Considerações sobre design

- Por padrão, a AWS Control Tower nomeia a conta sob a OU de Segurança como Conta de Auditoria. Você pode renomear a conta durante a configuração da AWS Control Tower.
- 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 exigir 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 deveres, menor privilégio e potencial simplicidade das atribuições de equipes. Se você estiver usando o AWS Control Tower, isso restringe a criação de contas adicionais da AWS sob a OU de segurança.

ador delegado ado ado ado ado ado ado ado ado ado ado

A conta do Security Tooling serve como conta de administrador para serviços de segurança que são gerenciados em uma estrutura de administrador/membro em todas as contas da AWS. Conforme mencionado anteriormente, isso é feito por meio da funcionalidade de administrador delegado do AWS Organizations. Os serviços do AWS SRA que atualmente oferecem suporte ao administrador delegado incluem AWS Config, AWS Firewall Manager, Amazon GuardDuty, AWS IAM Access Analyzer, Amazon Macie, AWS Security Hub, AWS Detective, AWS Audit Manager, Amazon Inspector e AWS Systems Manager. Sua equipe de segurança gerencia os recursos de segurança desses serviços e monitora quaisquer eventos ou descobertas específicos de segurança.

O IAM Identity Center oferece suporte à administração delegada a uma conta de membro. O AWS SRA usa a conta do Shared Services como a conta de administrador delegado do IAM Identity Center, conforme explicado posteriormente na seção do IAM Identity Center (p. 55) da conta do Shared Services.

AWS Security Hub

O AWS Security Hub fornece uma visão abrangente do estado de sua segurança na AWS e ajuda você a verificar o ambiente de acordo com os padrões e as melhores práticas do setor de segurança. O Security Hub coleta dados de segurança de todos os serviços integrados da AWS, produtos terceirizados suportados e outros produtos de segurança personalizados que você pode usar. Ele ajuda você a monitorar e analisar continuamente suas tendências de segurança e identificar os problemas de segurança de prioridade mais alta.

O Security Hub se integra ao AWS Organizations para simplificar o gerenciamento da postura de segurança em todas as suas contas existentes e future em sua organização da AWS. A conta de administrador delegado do Security Hub (nesse caso, Security Tooling) tem o Security Hub ativado automaticamente e pode escolher as contas da AWS a serem habilitadas como contas de membros. A conta de administrador delegado do Security Hub também pode visualizar descobertas, ver insights e controlar detalhes de todas as contas de 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 oferece suporte a integrações com vários serviços da AWS. Amazon GuardDuty, AWS Config, Amazon Macie, AWS IAM Access Analyzer, AWS Firewall Manager, Amazon Inspector e AWS Systems Manager Patch Manager podem enviar descobertas para o Security Hub. Além disso, você pode passar do Security Hub para o Amazon Detective para investigar uma GuardDuty descoberta da Amazon. O Security Hub recomenda alinhar as contas do administrador delegado para esses serviços (onde eles existirem) para uma integração mais fácil. Por exemplo, se você não alinhar as contas de administrador entre o Detective e o Security Hub, passar das descobertas para o Detective não funcionará.

Você pode usar o Security Hub com o recurso Network Access Analyzer do Amazon VPC para ajudar a monitorar continuamente a conformidade de sua configuração de rede da 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 o post do blog da AWS Verificação contínua da conformidade da rede usando o Amazon VPC Network Access Analyzer e o AWS Security Hub.

Além do monitoramento, o Security Hub 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. Mais discussões e exemplos estão disponíveis nessas duas postagens do blog da AWS: Automated Response and Remediation with AWS Security Hub e Como implantar a solução da AWS para resposta e remediação automatizadas do Security Hub.

O Security Hub usa regras do AWS Config vinculadas a serviços para realizar a maioria de suas verificações de segurança para controles. Para dar suporte a esses controles, o AWS Config deve estar ativado em todas as contas, incluindo a conta do administrador (ou administrador delegado) e as contas dos membros, em cada região da AWS em que o Security Hub está ativado.

Considerações sobre design

- Além das regras específicas e gerenciadas do AWS Config que o Security Hub usa, você pode usar a automação para importar outras regras do AWS Config para o Security Hub para que suas regras do AWS Config apareçam junto com suas outras descobertas de segurança. Isso permite que você use com mais facilidade as regras do AWS Config para ajudar a garantir a conformidade contínua em todas as suas contas da AWS. Para obter mais informações, consulte a postagem de blog Como importar avaliações de regras do AWS Config como descobertas no Security Hub.
- Se um padrão de conformidade, como o PCI-DSS, já estiver presente no Security Hub, o serviço de 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 conformidade do AWS Config oferecem uma maneira simplificada de fazer essa personalização. (Para obter mais informações sobre o AWS Config e pacotes de conformidade, consulte a seção AWS Config (p. 35).)

AWS GuardDuty

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

GuardDuty está habilitado em todas as contas por meio do AWS Organizations, e todas as descobertas podem ser visualizadas e acionadas pelas equipes de segurança GuardDuty apropriadas na conta do administrador delegado (nesse caso, a conta do Security Tooling).

Quando o AWS Security Hub está ativado, GuardDuty as descobertas fluem automaticamente para 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, que GuardDuty fornecem links do console que redirecionam você de uma descoberta selecionada para uma página do Detective que contém um conjunto selecionado de visualizações para investigar essa descoberta. Por exemplo, você também pode se integrar GuardDuty EventBridge à Amazon para automatizar as melhores práticas GuardDuty, como automatizar respostas a novas GuardDuty descobertas.

AWS Config

O AWS Config é um serviço que permite avaliar, auditar e verificar as configurações de recursos suportados pela AWS em suas contas da AWS. O AWS Config monitora e registra continuamente as configurações de recursos da AWS e avalia automaticamente as configurações registradas em relação às configurações desejadas. Você também pode integrar o AWS Config com outros serviços para fazer o trabalho pesado em pipelines automatizados de auditoria e monitoramento. Por exemplo, o AWS Config pode monitorar alterações em segredos individuais no AWS Secrets Manager.

O AWS Config deve estar habilitado para cada conta de membro na organização da AWS e para cada região da AWS que contenha os recursos que você deseja proteger. Você pode gerenciar centralmente (por exemplo, criar, atualizar e excluir) as regras do AWS Config em todas as contas da sua organização da AWS. Na conta de administrador delegado do AWS Config, você pode implantar um conjunto comum de regras do AWS Config em todas as contas e especificar contas nas quais as regras do AWS Config não devem ser criadas. A conta de administrador delegado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ada Use as APIs da conta de administrador delegado para impor a governança, garantindo que as regras subjacentes do AWS Config não sejam modificáveis pelas contas de membros da sua organização da AWS.

Um pacote de conformidade é uma coleção de regras e ações de remediação do AWS Config que podem ser implantadas como uma única entidade em uma conta e uma região, ou em uma organização no AWS Organizations. Os pacotes de conformidade são criados com a criação de um modelo YAML que contém a lista de regras gerenciadas ou personalizadas e ações de remediação gerenciadas ou gerenciadas pelo AWS Config. Para começar a avaliar seu ambiente da AWS, use um dos exemplos de modelos de pacote de conformidade.

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

As regras do AWS Config podem ser usadas em conjunto com o AWS Systems Manager para remediar recursos não compatíveis de forma eficaz. Você usa o AWS Systems Manager Explorer para reunir o

status de conformidade das regras do AWS Config em suas contas da AWS nas regiões da AWS e, em seguida, usa os documentos do Systems Manager Automation (runbooks) para resolver suas regras não compatíveis do AWS Config. Para obter detalhes sobre a implementação, consulte a postagem do blog Corrija regras não compatíveis do AWS Config com os runbooks do AWS Systems Manager Automation.

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

Consideração do design

- O AWS Config transmite notificações de alteração de configuração e conformidade para a Amazon EventBridge. Isso significa que você pode usar os recursos de filtragem nativa do EventBridge para filtrar eventos do AWS Config para que você possa encaminhar tipos específicos de notificações para destinos específicos. Por exemplo, você pode enviar notificações de conformidade de regras ou tipos de recursos específicos para endereços de e-mail específicos ou encaminhar 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 a postagem de blog: AWS Config best practices.

Amazon Macie

O Amazon Macie é um serviço de segurança e privacidade de dados totalmente gerenciado que usa machine learning e comparação de padrões para detectar e ajudar a proteger seus dados confidenciais na AWS. Você precisa entender o tipo e a classificação dos dados que sua carga de trabalho está processando para garantir que os controles apropriados sejam aplicados. O Macie automatiza a descoberta de dados confidenciais em grande escala. Com o Macie, você pode realizar várias tarefas de descoberta de conteúdo confidencial e classificação de dados em objetos no Amazon S3. O Macie está habilitado em todas as contas por meio do AWS Organizations. Os diretores que têm as permissões apropriadas na conta de 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 que pertencem a contas de membros e visualizar todas as conclusões de políticas de todas as contas de membros. As descobertas de dados confidenciais só podem ser visualizadas pela conta que criou a tarefa de descobertas confidenciais. Para obter mais informações, consulte Gerenciamento de várias contas no Amazon Macie na documentação do Macie.

As descobertas de Macie fluem para o AWS Security Hub para análise e análise. A Macie também se integra EventBridge à Amazon para facilitar respostas automatizadas às 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 do AWS Key Management Service (AWS KMS) que você gerencia, você poderá adicionar a função vinculada ao serviço Macie como usuário-chave a essa chave do KMS para permitir que o Macie escaneie os dados.
- O Macie é otimado para escanear objetos no Amazon S3. Como resultado, qualquer tipo de objeto compatível com o 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 do Amazon Relational Database Service (Amazon RDS) ou bancos de dados 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 avaliado por Macie.

AWS IAM Access Analyzer

O AWS IAM Access Analyzer ajuda você a identificar os recursos em sua organização e suas contas da AWS, como buckets do Amazon S3 ou funções do IAM, que são compartilhados com uma entidade externa. Esse controle de detetive ajuda você a identificar o acesso não intencional aos seus dados e recursos, o que é um risco de segurança.

O Access Analyzer é implantado na conta do Security Tooling por meio da funcionalidade de administrador delegado no AWS Organizations. O administrador delegado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ados As descobertas do Access Analyzer fluem automaticamente para o Security Hub. O Access Analyzer também envia um evento EventBridge para cada descoberta gerada, quando o status de uma descoberta existente é alterada e quando uma descoberta é excluída. EventBridge pode direcionar ainda mais esses eventos para fluxos de notificação ou remediação.

Consideração do design

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

AWS Firewall Manager

O AWS Firewall Manager ajuda a proteger sua rede simplificando suas tarefas de administração e manutenção para AWS WAF, AWS Shield Advanced, grupos de segurança Amazon VPC, AWS Network Firewall e Route 53 Resolver DNS Firewall em várias contas e recursos. Com o Firewall Manager, você configura as regras de firewall do AWS WAF, as proteções do Shield Advanced, os grupos de segurança da Amazon VPC, os firewalls do AWS Network Firewall e as associações de grupos de regras do DNS Firewall apenas 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 sua organização AWS 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 recursos (indicados por tags) devem ser incluídos ou excluídos. Você pode criar configurações granulares e flexíveis e, ao mesmo tempo, escalar 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 por meio do AWS Organizations, e a configuração e o gerenciamento são realizados pelas equipes de segurança apropriadas na conta do administrador delegado do Firewall Manager (nesse caso, a conta do Security Tooling).

Você deve habilitar o AWS Config para cada região da AWS que contém os recursos que você deseja proteger. Se você não quiser habilitar o AWS Config para todos os recursos, você deve habilitá-lo para recursos associados ao tipo de política do Firewall Manager que você usa. Quando você usa o AWS Security Hub e o Firewall Manager, o Firewall Manager envia automaticamente suas descobertas para o Security Hub. 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. Ao configurar uma política do Firewall Manager para o AWS WAF, você pode ativar centralmente o registro em listas de controle de acesso à web (ACLs da web) para todas as contas no escopo e centralizar os registros em uma única conta.

Consideração do design

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

Amazon EventBridge

Amazon EventBridge é um serviço de barramento de eventos sem servidor que facilita a conexão de aplicações a dados de diversas origens. 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 da AWS. Por exemplo, ao vincular as regras do AWS Config e o Security Hub EventBridge, você cria um pipeline flexível e automatizado para rotear dados de segurança, gerar alertas e gerenciar ações para resolver problemas. GuardDuty

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 respondentes individuais do AWS Lambda, que tomam as medidas apropriadas. Por exemplo, em determinadas circunstâncias, talvez você queira usar EventBridge para rotear uma descoberta pública de bucket do S3 para um respondente do Lambda que corrige a política do bucket e remove as permissões públicas. Esses respondentes podem ser integrados aos seus manuais de investigação e manuais para coordenar as atividades de resposta.
- A melhor prática 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 tíquetes, um sistema de bug/problema ou outro sistema de gerenciamento de eventos e informações de segurança (SIEM). Isso elimina o fluxo de trabalho dos e-mails e dos relatórios estáticos e ajuda você a rotear, escalar e gerenciar eventos ou descobertas. As capacidades flexíveis de roteamento do EventBridge são um poderoso facilitador dessa integração.

Amazon Detective

O Amazon Detective apoia sua estratégia de controle de segurança responsivo ao facilitar a análise, investigação e identificação rápida da causa raiz de descobertas de segurança ou atividades suspeitas para seus analistas de segurança. O Detective extrai automaticamente eventos baseados em tempo, como tentativas de login, chamadas de API e tráfego de rede, dos registros da AWS e dos CloudTrail registros de fluxo do Amazon VPC. O Detective consome esses eventos usando fluxos independentes de CloudTrail registros e registros de fluxo do Amazon VPC. O 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 fracassadas de login ou chamadas suspeitas de API.

Detective também ingere descobertas que são detectadas pela Amazon GuardDuty. Quando uma conta ativa Detective, ela se torna a conta de administrador para o gráfico de comportamento. Antes de tentar ativar o Detective, verifique se sua conta está cadastrada há GuardDuty pelo menos 48 horas. Se você não atender a esse requisito, não poderá ativar o Detective.

O Detective integra-se ao AWS Organizations. A conta do Org Management delega uma conta de membro como conta de administrador do Detective. No AWS SRA, essa é a conta do Security Tooling. A conta de administrador do Detective tem a capacidade de ativar automaticamente todas as contas de membros atuais na organização como contas de detetive e também adicionar novas contas de membros à medida que elas são adicionadas à organização da AWS. As contas de administrador de Detective também podem convidar contas de membros que atualmente não residem na organização da AWS, mas estão na mesma região, para 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.

Consideração do design

- Você pode navegar até Detective encontrando perfis nos consoles GuardDuty e no AWS Security Hub. 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 (GuardDuty ou do Security Hub). Se as contas principais forem as mesmas para os serviços, os links de integração funcionarão perfeitamente.

AWS Audit Manager

O AWS Audit Manager ajuda você a auditar continuamente o uso da AWS para simplificar a forma como você gerencia auditorias e a conformidade com 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 fonte 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 revisões de seus controles pelas partes interessadas.

Com o Audit Manager, você pode auditar estruturas pré-construídas, 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). Ele 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 evidências são automatizadas: evidências de verificação de conformidade do AWS Config e do AWS Security Hub, evidências de eventos de gerenciamento da AWS CloudTrail e evidências de configuração de chamadas de service-to-service API da AWS. Para evidências que não podem ser automatizadas, o Audit Manager permite que você faça o upload de evidências manuais.

Note

O Audit Manager auxilia na coleta de evidências relevantes para verificar a conformidade com padrões e regulamentos de conformidade específicos. Porém, essa tabela não verifica a conformidade. Portanto, as evidências coletadas por meio do Audit Manager podem não incluir detalhes de seus processos operacionais que são necessários para auditorias. O Audit Manager não substitui o aconselhamento jurídico ou os especialistas em conformidade. Recomendamos que você contrate os serviços de um avaliador terceirizado que seja certificado pela (s) estrutura (s) de conformidade com a (s) qual (is) você foi avaliado.

As avaliações do Audit Manager podem ser executadas em várias contas em suas organizações da AWS. O Audit Manager coleta e consolida evidências em uma conta de administrador delegado no AWS Organizations. Essa funcionalidade de auditoria é usada principalmente pelas equipes de auditoria interna e de conformidade e requer apenas acesso de leitura às suas contas da AWS.

Considerações sobre design

- O Audit Manager complementa outros serviços de segurança da AWS, como o Security Hub e o 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 ajuda você a supervisionar seus riscos e os pacotes de conformidade do AWS Config ajudam a gerenciar seus riscos. Os profissionais de auditoria que estão familiarizados com o modelo de três linhas desenvolvido pelo Institute of Internal Auditors (IIA) devem observar que essa combinação de 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 AWS Cloud Operations & Migrations.

- Para que o Audit Manager colete evidências do Security Hub, a conta de administrador delegado para ambos os serviços deve 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

O AWS Artifact é hospedado na conta do Security Tooling para delegar a funcionalidade de gerenciamento de artefatos de conformidade da conta do AWS Org Management. Essa delegação é importante porque recomendamos que você evite usar a conta do AWS Org Management para implantações, a menos que seja absolutamente necessário. Em vez disso, delegue implantações às 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 as equipes de segurança e conformidade, a conta do Security Tooling é designada como a conta de administrador delegado do AWS Artifact. Você pode usar os relatórios do AWS Artifact para baixar documentos de segurança e conformidade da AWS, como certificações ISO da AWS, Payment Card Industry (PCI) e relatórios de System and Organization Controls (SOC). Você pode restringir esse recurso somente às funções do AWS Identity and Access Management (IAM) pertencentes às suas equipes de auditoria e conformidade, para que elas possam baixar, analisar e fornecer esses relatórios aos auditores externos, conforme necessário. Além disso, você pode restringir funções específicas do IAM para ter acesso somente a relatórios específicos do AWS Artifact por meio de políticas do IAM. Para ver exemplos de políticas do IAM, consulte a documentação do AWS Artifact.

Consideração do design

- Se você optar por ter uma conta dedicada da AWS para equipes de auditoria e conformidade, poderá hospedar o AWS Artifact em uma conta de auditoria de segurança, que é separada da conta do Security Tooling. Os relatórios do AWS Artifact 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 durante todo o ciclo de vida de desenvolvimento do sistema e podem ser usados como evidência em auditorias e avaliações internas ou externas.

AWS KMS

O 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. O 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 de chaves. O AWS KMS pode ajudar a proteger seus dados com chaves de criptografia e assinatura, e pode ser usado tanto para criptografia do lado do servidor quanto para criptografia do lado do cliente por meio do AWS Encryption SDK. Para proteção e flexibilidade, o AWS KMS oferece suporte a três tipos de chaves: chaves gerenciadas pelo cliente, chaves gerenciadas pela AWS e chaves de propriedade da AWS. Chaves gerenciadas pelo cliente são chaves do AWS KMS disponíveis na sua conta da AWS que você cria, detém e gerencia. Chaves gerenciadas pela AWS KMS em sua conta que são criadas, gerenciadas e usadas em seu nome por um serviço da AWS integrado ao AWS KMS. Chaves de propriedade da AWS são uma coleção de chaves do AWS KMS que um serviço da AWS detém e gerencia para uso em várias contas da AWS. Para obter mais informações sobre o uso de chaves KMS, consulte a documentação do AWS KMS e os detalhes criptográficos do AWS KMS.

Uma opção de implantação é centralizar a responsabilidade do gerenciamento de chaves do KMS em uma única conta e, ao mesmo tempo, delegar a capacidade de usar chaves na conta do aplicativo por recursos do aplicativo usando uma combinação de políticas de chaves e do IAM. Essa abordagem é segura e fácil de gerenciar, mas você pode encontrar obstáculos devido aos limites de limitação do AWS KMS, aos limites do serviço de 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 permite que o AWS KMS resida em várias contas e permite que os responsáveis pela infraestrutura e pelas cargas de trabalho em uma conta específica gerenciem suas próprias chaves. Esse modelo oferece às 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 apenas uma conta da AWS e simplifica a emissão de relatórios, auditorias e outras tarefas relacionadas à conformidade. Em um modelo descentralizado, é importante implantar e aplicar barreiras de proteção para que as chaves descentralizadas sejam gerenciadas da mesma forma e o uso das chaves KMS seja auditado de acordo com as melhores práticas e políticas estabelecidas. Para obter mais informações, consulte o whitepaper AWS Key Management Service Best Practices. O AWS SRA recomenda um modelo de gerenciamento de chaves distribuído no qual as chaves KMS residam localmente na conta em que são usadas. Recomendamos que você evite usar uma única chave em uma conta para todas as funções criptográficas. Chaves podem ser criadas com base em requisitos de função e proteção de dados e para aplicar o princípio de privilégio mínimo. Em alguns casos, as permissões de criptografia seriam mantidas separadas das permissões de decodificação, e os administradores gerenciariam as funções do ciclo de vida, mas não conseguiriam criptografar nem descriptografar dados com as chaves que gerenciam.

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

CA privada da AWS

AWS Private Certificate Authority(CA privada da AWS) é um serviço de CA privado gerenciado que ajuda você a gerenciar com segurança o ciclo de vida de seus certificados TLS de entidade final privada para instâncias, contêineres, dispositivos de IoT e recursos locais do EC2. Ele permite comunicações TLS criptografadas para aplicativos em execução. Com oCA privada da AWS, é possível criar sua própria hierarquia de autoridades de certificação (uma CA raiz, por meio de CAs subordinadas, até certificados de entidade final) e emitir certificados com ela para autenticar usuários internos, computadores, aplicativos, serviços, servidores e outros dispositivos, e assinar código de computador. Os certificados emitidos por uma CA privada são confiáveis somente em sua organização da AWS, não na Internet.

Uma infraestrutura de chave pública (PKI) ou uma equipe de segurança pode ser responsável por gerenciar 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 automaticamente aos requisitos de certificados. O AWS SRA representa uma hierarquia centralizada de CA na qual a CA raiz é 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 com uma conta de aplicativo usando o AWS Resource Access Manager (AWS RAM). A RAM da AWS gerencia as permissões necessárias para o compartilhamento entre contas. Isso elimina a necessidade de uma CA privada em cada conta e fornece uma forma de implantação mais econômica. Para obter mais informações sobre o fluxo de trabalho e a implementação, consulte a postagem do blog Como usar a RAM da AWS para compartilhar suasCA privada da AWS contas cruzadas.

> Note
>
> O ACM também ajuda você a provisionar, gerenciar e implantar certificados TLS públicos para uso com os serviços da AWS. Para oferecer suporte a essa funcionalidade, o ACM precisa residir na conta da AWS que usaria o certificado público. Isso será discutido posteriormente neste guia, na seção Conta do aplicativo (p. 56).

Considerações sobre design

- Com o 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. ACA privada da AWS hierarquia deve seguir o design de PKI da sua organização. No entanto, lembre-se de que aumentar a hierarquia de 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 oferece benefícios que incluem controle de segurança granular apropriado a cada CA, delegação da CA subordinada a um aplicativo diferente, o que leva à divisão de tarefas administrativas, uso de CA com confiança revogável limitada, capacidade de definir diferentes períodos de validade e capacidade de impor limites de caminho. O ideal é que suas CAs raiz e subordinadas estejam em contas separadas da AWS. Para obter mais informações sobre como planejar uma hierarquia de CA usandoCA privada da AWS, consulte a CA privada da AWSdocumentação e a publicação do blog Como proteger umaCA privada da AWS hierarquia de escala corporativa para o setor automotivo e de manufatura.
- CA privada da AWSpode se integrar à sua hierarquia de CA existente, o que permite que você use a automação e a capacidade de integração nativa da AWS do ACM em conjunto com a raiz de confiança existente que você usa atualmente. Você pode criar uma CA subordinadaCA 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 principal externa naCA privada da AWS documentação.

Amazon Inspector

O Amazon Inspector é um serviço automatizado de gerenciamento de vulnerabilidades que verifica continuamente workloads do Amazon EC2 e do contêiner em busca de vulnerabilidades de software e exposição não intencional da rede.

O Amazon Inspector avalia continuamente seu ambiente durante todo o ciclo de vida de seus recursos, escaneando automaticamente os recursos sempre que você faz alterações neles. Os eventos que iniciam a redigitalização 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. Quando uma vulnerabilidade aberta é detectada, o Amazon Inspector calcula uma pontuação de risco do Amazon Inspector 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.

As descobertas de acessibilidade de rede do Amazon Inspector avaliam a acessibilidade de suas instâncias do EC2 de ou para bordas da VPC, como gateways de internet, conexões de emparelhamento de VPC ou redes privadas virtuais (VPNs) por meio de um gateway virtual. Essas regras ajudam a automatizar o monitoramento de suas redes da AWS e a identificar onde o acesso à rede às suas instâncias do EC2 pode estar configurado incorretamente 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.

Os agentes do AWS Systems Manager (SSM Agents) são necessários para a verificação de vulnerabilidades de instâncias do EC2. Não são necessários agentes para a acessibilidade de rede de instâncias EC2 ou verificação de vulnerabilidade de imagens de contêiner no Amazon Elastic Container Registry (Amazon ECR).

O Amazon Inspector é integrado AWS Organizations e oferece suporte à administração delegada. No AWS SRA., a conta Security Tooling é transformada em conta de administrador delegado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado ado

Considerações sobre design

- O Amazon Inspector se integra automaticamente ao AWS Security Hub quando os dois serviços estão habilitados. Você pode usar essa integração para enviar todas as descobertas do Amazon Inspector para o Security Hub, que então incluirá tais descobertas na análise feita sobre sua postura de segurança.
- O Amazon Inspector exporta automaticamente os resultados 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 chave KMS que o Amazon Inspector possa usar para criptografar descobertas e de um bucket do S3 com permissões que permitam ao Amazon Inspector fazer upload de objetos. EventBridge a integração permite monitorar e processar descobertas quase em tempo real como parte de seus fluxos de trabalho de segurança e conformidade existentes. EventBridge os eventos são publicados na conta de administrador delegado do Amazon Inspector, além da conta de membro da qual eles se originaram.

Implantação de serviços de segurança comuns em todas as contas da AWS

A seção Aplicar serviços de segurança em sua organização da AWS (p. 17), anteriormente nesta referência, destacou os serviços de segurança que protegem uma conta da AWS e observou que muitos desses serviços também podem ser configurados e gerenciados dentro 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 sua organização da AWS.

As trilhas CloudTrail organizacionais do Security Hub GuardDuty, do AWS Config, do Access Analyzer e da AWS aparecem em todas as contas. Os três primeiros oferecem suporte ao recurso de administrador delegado discutido anteriormente na seção Conta de gerenciamento, acesso confiável e administradores delegados (p. 12). CloudTrail atualmente usa um mecanismo de agregação diferente.

O repositório deGitHub código do AWS SRA fornece um exemplo de implementação para habilitar o Security Hub GuardDuty, o AWS Config, o Firewall Manager e as trilhas CloudTrail organizacionais em todas as suas contas, incluindo a conta do AWS Org Management.

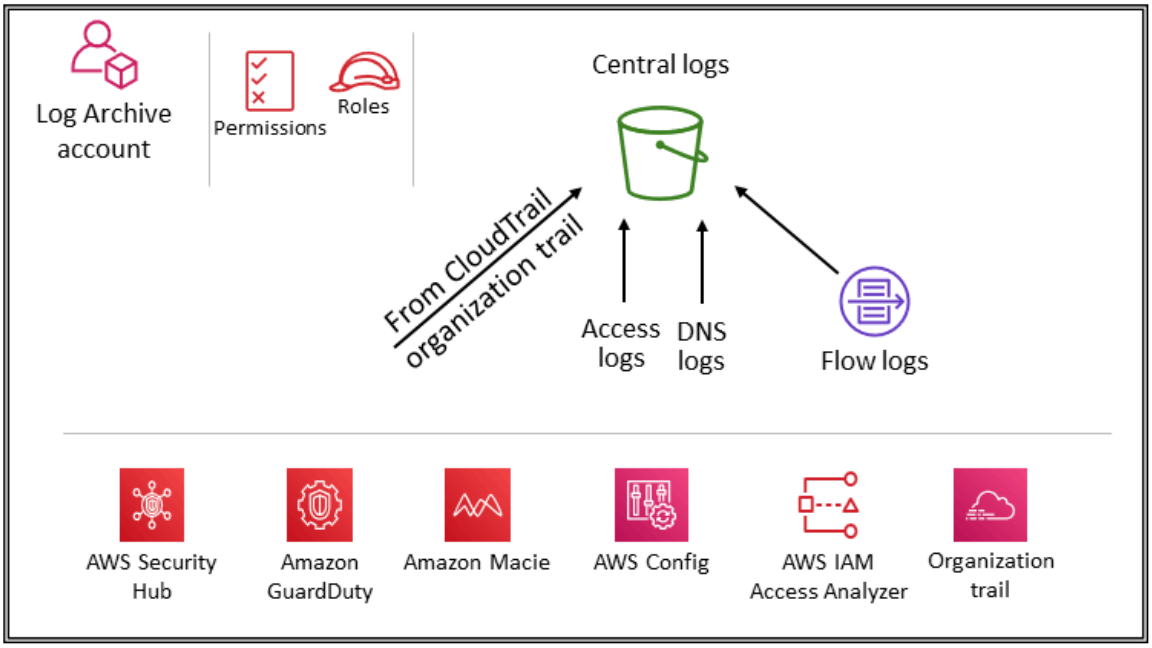
Considerações sobre design

- Configurações específicas da conta podem exigir serviços de segurança adicionais. Por exemplo, as contas que gerenciam buckets do S3 (as contas Application e Log Archive) também devem incluir o Amazon Macie e considerar ativar o registro de eventos de dados do CloudTrail 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 do EC2 ou imagens do Amazon ECR.
- Além dos serviços descritos anteriormente nesta seção, o AWS SRA inclui dois serviços focados em segurança, o AWS Detective e o AWS Audit Manager, que oferecem suporte à integração AWS Organizations e à funcionalidade do administrador delegado. No entanto, esses serviços não estão incluídos como parte dos serviços recomendados para a base de contas, 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, no início do seu projeto e, em seguida, desenvolvê-las usando serviços que fornecem recursos adicionais.

Security OU - Conta Log Archive

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

O diagrama a seguir ilustra os serviços de segurança da AWS 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 de identidades, mudanças na política do IAM e outras atividades críticas realizadas em recursos confidenciais. Os objetivos de segurança são simples: esse deve ser um armazenamento imutável, acessado somente por mecanismos controlados, automatizados e monitorados e criado para proporcionar 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 chave controlada do AWS KMS, use controles de detetive, como o AWS Config, para monitorar (alertar e corrigir) essa coleção de permissões em caso de alterações inesperadas.

Consideração do 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 log na conta do Log Archive. Com base em seus requisitos específicos de segurança e governança, talvez seja necessário filtrar os dados de registro operacional salvos nessa conta. Talvez você também precise especificar quem tem acesso aos dados de registro operacional na conta do Log Archive.

Tipos de registros

Os principais registros mostrados no AWS SRA incluem CloudTrail (trilha da organização), registros de fluxo do Amazon VPC, registros de acesso do Amazon CloudFront e do AWS WAF e registros de DNS do Amazon Route 53. Esses registros fornecem uma auditoria das ações tomadas (ou tentadas) por um usuário, função, serviço da AWS ou entidade de rede (identificada, 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 registro e melhores práticas de registro, consulte a documentação de segurança de cada serviço.

Amazon S3 como armazenamento central de registros

Muitos serviços da AWS registram informações no Amazon S3, seja por padrão ou exclusivamente. AWS CloudTrail, Amazon VPC Flow Logs, AWS Config e Elastic Load Balancing são alguns exemplos de serviços que registram informações no Amazon S3. Isso significa que a integridade do registro é alcançada por meio da integridade do objeto do S3; a confidencialidade do registro é obtida por meio dos controles de acesso ao objeto do S3; e a disponibilidade do registro 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 do S3 centralizado e dedicado que reside em uma conta dedicada, você pode gerenciar esses registros em apenas alguns buckets e impor rigorosos controles de segurança, acesso e separação de tarefas.

No AWS SRA, vêm os registros primários armazenados no Amazon S3 CloudTrail, então 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 automatizadas.

Por padrão, CloudTrail os registros nos buckets do S3 são criptografados pela criptografia no lado do S3 3 (SSE-S3) da 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 de segurança gerenciada adicional, você pode usar a criptografia no lado do servidor com chaves do AWS KMS que você gerencia (SSE-KMS) em todos os buckets de segurança do S3 3 3 3. Isso adiciona um segundo nível de controle de acesso. Para ler arquivos de log, um usuário deve ter permissões de leitura do Amazon S3 para o objeto do S3 e uma política ou função do IAM aplicada que permita que ele tenha permissões de decodificação de acordo com a política de chaves associada.

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

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

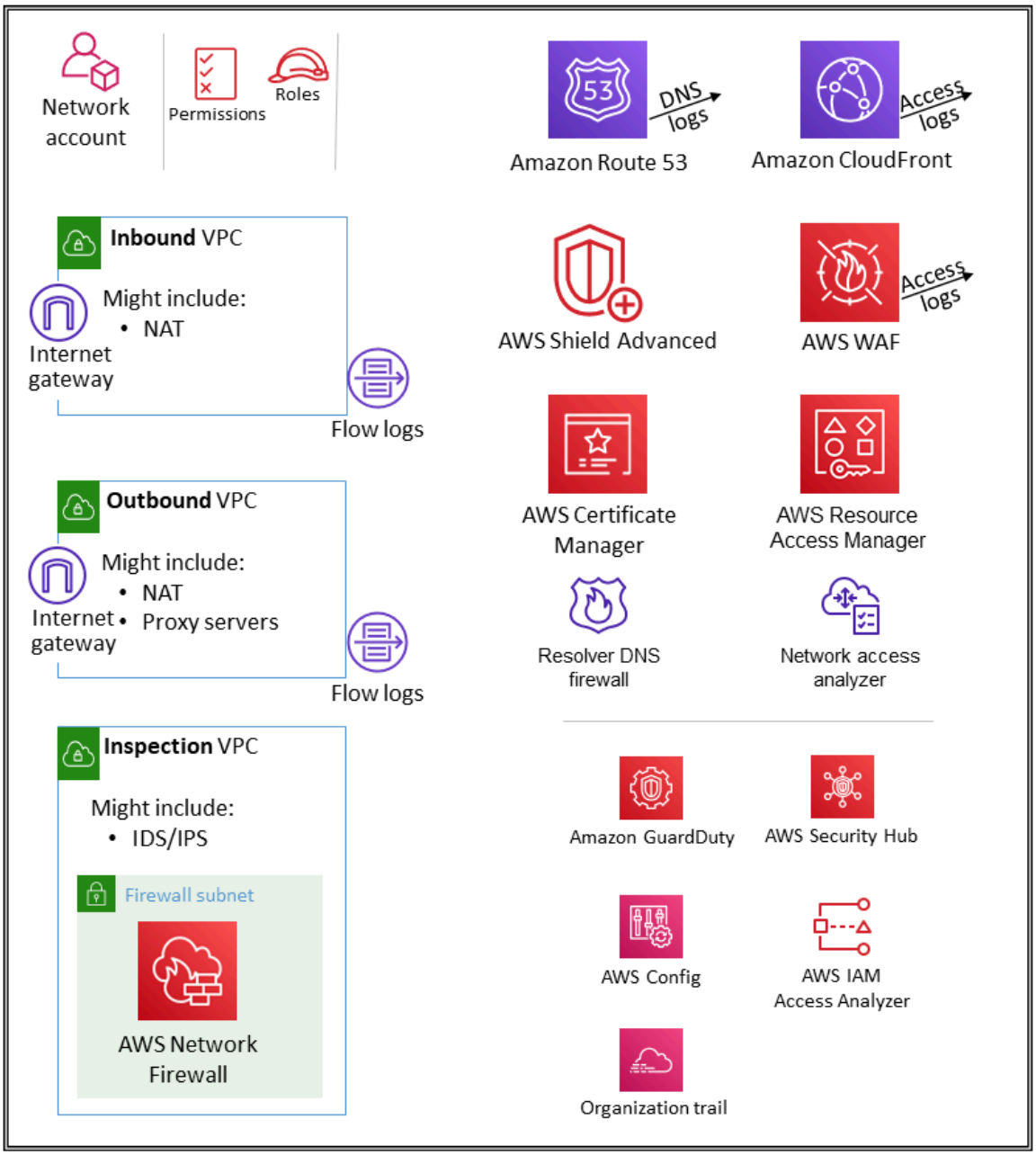
Use controles de detetive, como os fornecidos pelo AWS Config e pelo AWS IAM Access Analyzer, para monitorar (e alertar e corrigir) esse coletivo mais amplo de controles preventivos para mudanças inesperadas.

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

Infraestrutura OU - Conta de rede

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

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



A conta de rede gerencia o gateway entre seu aplicativo e a Internet em geral. É importante proteger essa interface bidirecional. A conta de rede isola os serviços, a configuração e a operação de rede das cargas de trabalho, da segurança e de outras infraestruturas de aplicativos individuais. Esse acordo não apenas

limita a conectividade, as permissões e o fluxo de dados, mas também suporta a separação de funções e o mínimo de privilégios para as equipes que precisam operar nessas contas. Ao dividir o fluxo de rede em nuvens privadas virtuais (VPCs) de entrada e saída separadas, você pode proteger a infraestrutura e o tráfego confidenciais contra acessos indesejados. A rede de entrada geralmente é considerada de maior risco e merece roteamento, monitoramento e possíveis mitigações de problemas. Essas contas de infraestrutura herdarão as barreiras de permissão da conta de gerenciamento da organização e da OU da infraestrutura. As equipes de rede (e segurança) gerenciam a maior parte da infraestrutura nessa conta.

Arquitetura de rede

Embora o design e as especificações da rede estejam além do escopo deste documento, recomendamos essas três opções de conectividade de rede entre as várias contas: VPC peering PrivateLink, AWS e AWS Transit Gateway. Considerações importantes na escolha entre elas são normas operacionais, orçamentos e necessidades específicas de largura de banda.

- emparelhamento de VPC – A maneira mais simples de conectar duas VPCs é usar o emparelhamento de VPC. Uma conexão permite conectividade bidirecional completa entre os VPCs. As VPCs que estão em contas e regiões da AWS separadas também podem ser emparelhadas. Em grande escala, quando você tem dezenas a centenas de VPCs, interconectá-las com o emparelhamento resulta em uma malha de centenas a milhares de conexões de emparelhamento, 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 as VPCs é controlado e protegido e o número de VPCs a serem conectadas é menor que 10 (para permitir o gerenciamento individual de cada conexão).
- AWS PrivateLink – PrivateLink fornece conectividade privada entre VPCs, serviços e aplicativos. É possível criar sua própria aplicação na VPC e configurá-la como um serviço PrivateLink habilitado pelo (chamado de serviço de endpoint). Outras entidades principais da AWS podem criar uma conexão da VPC para o serviço de endpoint usando o endpoint da VPC de interface ou um endpoint do Gateway Load Balancer, dependendo do tipo de serviço. Quando você usa PrivateLink, o tráfego do serviço não passa por uma rede roteável publicamente. Use PrivateLink quando você tiver uma configuração cliente-servidor na qual você deseja dar a uma ou mais VPCs de consumidores acesso 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 nas duas VPCs têm endereços IP sobrepostos, pois PrivateLink usa interfaces de rede elásticas dentro da 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 conectar VPCs e redes locais como um serviço totalmente gerenciado sem exigir que você provisione dispositivos virtuais. A AWS gerencia a alta disponibilidade e escalabilidade. Um gateway de trânsito é um recurso regional e pode conectar milhares de VPCs na mesma região da AWS. Você pode conectar sua conectividade híbrida (conexões VPN e AWS Direct Connect) a um único gateway de trânsito, consolidando e controlando toda a configuração de roteamento da sua organização da AWS em um só lugar. Um gateway de trânsito resolve 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, mas necessidades específicas de custo, largura de banda e latência podem tornar o emparelhamento de VPC mais adequado às suas necessidades.

VPC de entrada (entrada)

O VPC de entrada tem como objetivo aceitar, inspecionar e rotear conexões de rede iniciadas fora do aplicativo. Dependendo das especificidades do aplicativo, você pode esperar ver alguma tradução de endereços de rede (NAT) nessa VPC. Os registros de fluxo dessa VPC são capturados e armazenados na conta do Log Archive.

VPC de saída (saída)

A VPC de saída se destina a lidar com conexões de rede iniciadas de dentro do aplicativo. Dependendo das especificidades do aplicativo, você pode esperar ver tráfego NAT, endpoints de VPC específicos para serviços da AWS e hospedagem de endpoints de API externos nessa VPC. Os registros de fluxo dessa VPC são capturados e armazenados na conta do Log Archive.

Inspeção VPC

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

AWS Network Firewall

O AWS Network Firewall é um serviço de firewall de rede gerenciado e altamente disponível para sua VPC. Ele permite que você implante e gerencie sem esforço a inspeção em estado, a prevenção e detecção de intrusões e a filtragem da web para ajudar a proteger suas redes virtuais na AWS. Para obter mais informações sobre como configurar o Network Firewall, consulte a postagem do blog AWS Network Firewall — New Managed Firewall Service in 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 dentro da zona, exceto a sub-rede em que ela está localizada. Dependendo do caso de uso e do modelo de implantação, a sub-rede do firewall pode ser pública ou privada. O firewall é totalmente transparente ao fluxo de tráfego e não executa a conversão de endereços de rede (NAT). Ele preserva o endereço 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 de 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 de rede ao enviar registros para o Amazon Simple Storage Service (Amazon S3) e para o Amazon Kinesis Data Firehose. CloudWatch O Network Firewall é interoperável com sua abordagem de segurança existente, incluindo tecnologias de parceiros da AWS. Você também pode importar conjuntos de regras Suricata existentes, que podem ter sido escritos internamente ou adquiridos externamente de fornecedores terceirizados ou plataformas de código aberto.

No AWS SRA, o Network Firewall 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

- O AWS Firewall Manager oferece suporte ao Network Firewall, para que você possa configurar e implantar centralmente as regras do Network Firewall em toda a sua organização. (Para obter detalhes, consulte as políticas do AWS Network Firewall na documentação da AWS.) 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 contém sub-redes públicas. Ao mesmo tempo, qualquer alteração no conjunto de regras configurado centralmente é automaticamente atualizada posteriormente nos firewalls de Network Firewall implantados.
- Há vários modelos de implantação disponíveis com o Network Firewall. O modelo certo depende de seu caso de uso e de seus requisitos. Os exemplos incluem:
  - Um modelo de implantação distribuída em que o Network Firewall é implantado em VPCs individuais.

  - Um modelo de implantação centralizada em que o Network Firewall é implantado em uma VPC centralizada para tráfego leste-oeste (VPC para VPC) ou norte-sul (entrada e saída da Internet, local).
  - Um modelo de implantação combinado em que o Network Firewall é implantado em uma VPC centralizada para tráfego leste-oeste e um subconjunto do tráfego norte-sul.
- Como prática recomendada, não use a sub-rede do Network Firewall para implantar nenhum serviço da. Isso ocorre porque o Network Firewall não pode inspecionar o tráfego de fontes ou destinos dentro da sub-rede do firewall.

Network Access Analyzer

O Network Access Analyzer é um recurso do Amazon VPC que identifica o acesso à rede não intencional aos seus recursos. Você pode usar o Network Access Analyzer para validar a segmentação da rede, identificar recursos acessíveis pela Internet ou acessíveis somente a partir de intervalos de endereços IP confiáveis e validar se você tem controles de rede apropriados em todos os caminhos da rede.

O Network Access Analyzer usa algoritmos de raciocínio automatizados para analisar os caminhos de rede que um pacote pode seguir entre recursos em uma rede da AWS e produz descobertas de caminhos que correspondem ao escopo de acesso à rede definido. O Network Access Analyzer 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 do Aplicativo. Tanto o Network Access Analyzer quanto o Network Reachability usam a tecnologia mais recente da iniciativa AWS Provable Security e aplicam essa tecnologia com diferentes áreas de foco. O pacote Network Reachability se concentra especificamente nas instâncias do EC2 e em sua acessibilidade à Internet.

A conta de rede define a infraestrutura de rede crítica que controla o tráfego de entrada e saída do seu ambiente da AWS. Esse tráfego precisa ser rigorosamente monitorado. 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.

Consideração de design

- O Network Access Analyzer é um recurso do Amazon VPC e pode ser usado em qualquer conta da AWS que tenha uma VPC. Os administradores de rede podem obter funções de IAM com escopo rígido e entre contas para validar se os caminhos de rede aprovados são aplicados em cada conta da AWS.

AWS Certificate Manager

O AWS Certificate Manager (ACM) permite provisionar, gerenciar e implantar certificados TLS públicos e privados para uso com serviços da AWS e seus recursos internos conectados. Com o ACM, você pode solicitar rapidamente um certificado, implantá-lo em recursos da AWS integrados ao ACM, como balanceadores de carga Elastic Load Balancing, CloudFront distribuições da Amazon e APIs no Amazon API Gateway, e deixar o ACM lidar com as renovações de certificados. Não é necessário gerar um key pair ou uma solicitação de assinatura de certificado (CSR), enviar uma CSR para 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 CAs de terceiros e implantá-los com serviços integrados do ACM. Quando você usa o ACM para gerenciar certificados, as chaves privadas dos certificados são protegidas e armazenadas com segurança usando as melhores práticas de criptografia e gerenciamento

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 os visualizadores CloudFront e. Para obter mais informações, consulte a CloudFront documentação da.

Consideração de design

- Para certificados externos, o ACM deve residir na mesma conta dos recursos para os quais fornece certificados. Os certificados não podem ser compartilhados em todas as contas da.

AWS WAF

O AWS WAF é um firewall de aplicação Web que permite monitorar solicitações HTTP e HTTPS que são encaminhadas para uma CloudFront distribuição da Amazon, uma API REST do Amazon API Gateway, para um Application Application Load Balancer ou uma API GraphQL do AWS AppSync GraphQL. O AWS WAF também permite que você controle o acesso ao seu conteúdo. Com base nas condições que você especificar, como de quais endereços IP se originam as solicitações ou os valores das query strings, o serviço responde às solicitações com o conteúdo solicitado ou com um código de status HTTP 403 (Proibido).

No AWS SRA, o AWS WAF é usado na conta de rede, porque protege CloudFront.

Considerações sobre design

- CloudFront fornece recursos que aprimoram a funcionalidade do AWS WAF e fazem com que os dois serviços funcionem melhor juntos.
- Você pode usar o AWS WAF, AWS Firewall Manager e o AWS Shield juntos para criar uma solução de segurança abrangente. Tudo começa com o AWS WAF. Você pode automatizar e depois simplificar o gerenciamento do AWS WAF usando o Firewall Manager. O Shield Advanced fornece recursos adicionais além do AWS WAF, como suporte dedicado da Equipe de Resposta Distribuída de Negação de Serviço (DDoS) (DRT) e relatórios avançados. Se você quiser um controle granular sobre a proteção que é adicionada aos seus recursos, o AWS WAF sozinho é a escolha certa. Se você quiser usar o AWS WAF em várias contas, acelerar sua configuração do AWS WAF ou automatizar a proteção de novos recursos, use o Firewall Manager com o AWS WAF. Por fim, se você possui sites de alta visibilidade ou está propenso a eventos maliciosos frequentes de DDoS, considere comprar os recursos adicionais que o AWS Shield Advanced oferece.

Amazon Route 53

O Amazon Route 53 é um web service de Domain Name System (DNS) altamente disponível e dimensionável. É possível 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 serviço de DNS para mapear nomes de domínio para suas instâncias do EC2, buckets do S3, CloudFront distribuições e outros recursos da AWS. A natureza distribuída de nossos servidores DNS ajuda a garantir que seus usuários finais sejam roteados para seu aplicativo de forma consistente. Recursos como o fluxo de tráfego e o controle de roteamento do Route 53 ajudam a melhorar a confiabilidade com um failover configurado de forma simples para redirecionar seus usuários para um local alternativo se o endpoint principal do aplicativo ficar indisponível. O Route 53 Resolver fornece DNS recursivo para sua VPC e redes locais por meio do AWS Direct Connect ou uma VPN gerenciada pela AWS.

Ao usar o serviço AWS Identity and Access Management (IAM) com o Route 53, você obtém um controle refinado sobre quem pode atualizar seus dados de DNS. Você pode ativar a assinatura de DNS Security Extensions (DNSSEC) para permitir que os resolvedores DNS validem que uma resposta DNS veio do Route 53 e não foi adulterada.

O Route 53 Resolver DNS Firewall fornece proteção para solicitações DNS de saída de suas VPCs. Essas solicitações são roteadas por meio do 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 que você sabe que são incorretos e permitir que todas as outras consultas passem. Como alternativa, você pode negar acesso a todos os domínios, exceto aqueles em que você confia explicitamente. Você também pode usar o Firewall DNS para bloquear solicitações de resolução para recursos em zonas hospedadas privadas (compartilhadas ou locais), incluindo nomes de endpoints da VPC. Ele também pode bloquear solicitações de nomes de instâncias públicas ou privadas do EC2.

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 do DNS.

Consideração de design

- O Firewall DNS e o AWS Network Firewall oferecem filtragem de nomes de domínio, mas para diferentes tipos de tráfego. É possível usar o Firewall DNS e o Network Firewall juntos para configurar a filtragem baseada em domínio para o tráfego da camada de aplicação em dois caminhos de rede diferentes.
  - O Firewall DNS fornece filtragem para consultas de DNS de saída que passam pelo Route 53 Resolver a partir de aplicações dentro de suas 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 da camada de rede e da camada de aplicação, mas não tem visibilidade nas consultas feitas pelo Route 53 Resolver.

Amazônia CloudFront

CloudFront A Amazon é uma rede segura de entrega de conteúdo (CDN) que fornece proteção em nível de rede e de aplicativo. Você pode entregar seu conteúdo, APIs ou aplicativos usando certificados SSL/TLS, e os recursos SSL avançados são ativados automaticamente. Você pode usar o AWS Certificate Manager (ACM) para criar um certificado TLS personalizado e impor comunicações HTTPS entre os visualizadores e CloudFront, conforme descrito anteriormente na seção ACM (p. 49). Além disso, você pode exigir que as comunicações CloudFront entre sua origem personalizada implementem end-to-end criptografia em trânsito. Para esse cenário, você precisará instalar um certificado TLS no seu servidor de origem. Se a origem for um balanceador de carga do ELB, você poderá usar um certificado gerado pelo ACM ou um certificado validado por uma CA terceirizada e importado no ACM. Se os endpoints do site bucket do S3 servirem como origem, você não poderá configurar o CloudFront para usar HTTPS com sua origem porque o Amazon S3 não é compatível com HTTPS para endpoints de site. (No entanto, você ainda pode exigir HTTPS entre os visualizadores CloudFront e.) Para todas as outras origens que suportam a instalação de certificados HTTPS, você deve usar um certificado assinado por uma CA terceirizada reconhecida.

Ao usar CloudFront como CDN, você pode restringir o acesso ao conteúdo usando esses recursos:

- Ao usar URLs assinados e cookies assinados, você pode oferecer suporte à autenticação por token para restringir o acesso somente a visualizadores autenticados.
- Ao usar o recurso de restrição geográfica, você pode trabalhar para impedir que usuários em localizações geográficas específicas acessem o conteúdo por meio do qual você está distribuindo CloudFront.
- Você pode usar o recurso de identidade de acesso de origem (OAI) para restringir o acesso a um bucket do S3 para ser acessado somente a partir de CloudFront.

No AWS SRA, a Amazon CloudFront é usada dentro da conta de rede, porque essa conta fornece a infraestrutura de rede necessária para que as cargas de trabalho se comuniquem fora da AWS.

Considerações sobre design

- CloudFront, o AWS Shield, o AWS WAF e o Amazon Route 53 trabalham perfeitamente juntos para criar um perímetro de segurança flexível em camadas contra vários tipos de eventos não autorizados, incluindo ataques de DDoS na rede e na camada de aplicativos. CloudFront fornece recursos que aprimoram a funcionalidade do AWS WAF e fazem com que os dois trabalhem melhor juntos. Para obter mais informações, consulte Como o AWS WAF funciona com os CloudFront recursos da Amazon na documentação da AWS.
- Quando você entrega conteúdo da web por meio de um CDN CloudFront, como, a melhor prática é evitar que as solicitações do espectador ignorem o CDN e acessem seu conteúdo de origem diretamente. Para obter mais informações, consulte a postagem de blog Como aprimorar a segurança de CloudFront origem da Amazon com o AWS WAF e o AWS Secrets Manager.
- Talvez você também queira avaliar uma arquitetura distribuída em que toda a infraestrutura de rede necessária para que suas cargas de trabalho se comuniquem fora da AWS resida localmente na conta do aplicativo. Isso simplifica a arquitetura e o roteamento da rede e ajudaria a reduzir custos ao não exigir taxas de entrada/saída entre contas. Em uma arquitetura distribuída, você precisa impor uma forte supervisão de segurança para exercer controles de segurança em todos os caminhos da rede.

AWS Shield

O AWS Shield é um serviço gerenciado de proteção contra DDoS que protege aplicativos que são executados na AWS. O Shield fornece detecção contínua e mitigações automáticas em linha que minimizam o tempo de inatividade e a latência dos aplicativos, portanto, não há necessidade de contratar o AWS Support para se beneficiar da proteção contra DDoS.

No AWS SRA, o AWS Shield Advanced está configurado para proteger a Route 53 CloudFront e.

Consideração de design

- Existem dois níveis de escudo: Shield Standard e Shield Advanced. Todos os clientes da AWS se beneficiam das proteções automáticas do Shield Standard sem custo adicional. O Shield Standard fornece proteção contra os eventos de infraestrutura mais comuns e frequentes (camadas 3 e 4). O Shield Standard usa filtragem determinística de pacotes e modelagem de tráfego baseada em prioridade para mitigar automaticamente os ataques básicos da camada de rede. O Shield Advanced fornece mitigações automáticas mais sofisticadas para eventos não autorizados que visam seus aplicativos executados em recursos protegidos do Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB) CloudFront, Amazon, AWS Global Accelerator e Route 53. O Shield Advanced registra métricas que você pode monitorar na Amazon CloudWatch. (Para obter mais informações, consulte as métricas e alarmes do AWS Shield Advanced na documentação da AWS.) Se você possui sites de alta visibilidade ou está propenso a ataques frequentes de DDoS, considere os recursos adicionais que o Shield Advanced oferece.

AWS RAM

O AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar com segurança os recursos da AWS que você cria em uma conta da AWS com outras contas da AWS. A RAM da AWS 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, ao mesmo tempo, aproveita o isolamento administrativo e

de cobrança e reduz o escopo dos benefícios de contenção de impactos fornecidos por uma estratégia de várias contas. Se sua conta for gerenciada pela AWS Organizations, a AWS RAM permite que você compartilhe recursos com todas as contas da organização ou somente com as contas dentro de uma ou mais unidades organizacionais (OUs) especificadas. Você também pode compartilhar com contas específicas da AWS por ID da conta, independentemente de a conta fazer parte de uma organização. Você também pode compartilhar alguns tipos de recursos compatíveis com funções e usuários específicos do IAM.

A RAM da AWS 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 a RAM da AWS, os proprietários de um recurso podem ver quais diretores têm acesso aos recursos individuais que eles compartilharam. As entidades do IAM podem recuperar a lista de recursos compartilhados diretamente com elas, o que não podem fazer com os recursos compartilhados pelas políticas de recursos do IAM. Se a RAM da AWS for usada para compartilhar recursos fora da sua organização da AWS, 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.

A RAM da AWS é invocada e gerenciada pelo proprietário do recurso, na conta em que o recurso compartilhado é implantado. Um caso de uso comum da RAM da AWS ilustrado no AWS SRA é que os administradores de rede compartilhem sub-redes VPC e gateways de trânsito com toda a organização da AWS. Isso fornece a capacidade de dissociar as funções de gerenciamento de contas e redes da AWS e ajuda a realizar a separação de tarefas. Para obter mais informações sobre compartilhamento de VPCs, consulte a publicação do blog da AWS VPC sharing: A new approach to multiple accounts and VPC management, e o whitepaper da infraestrutura de rede da AWS.

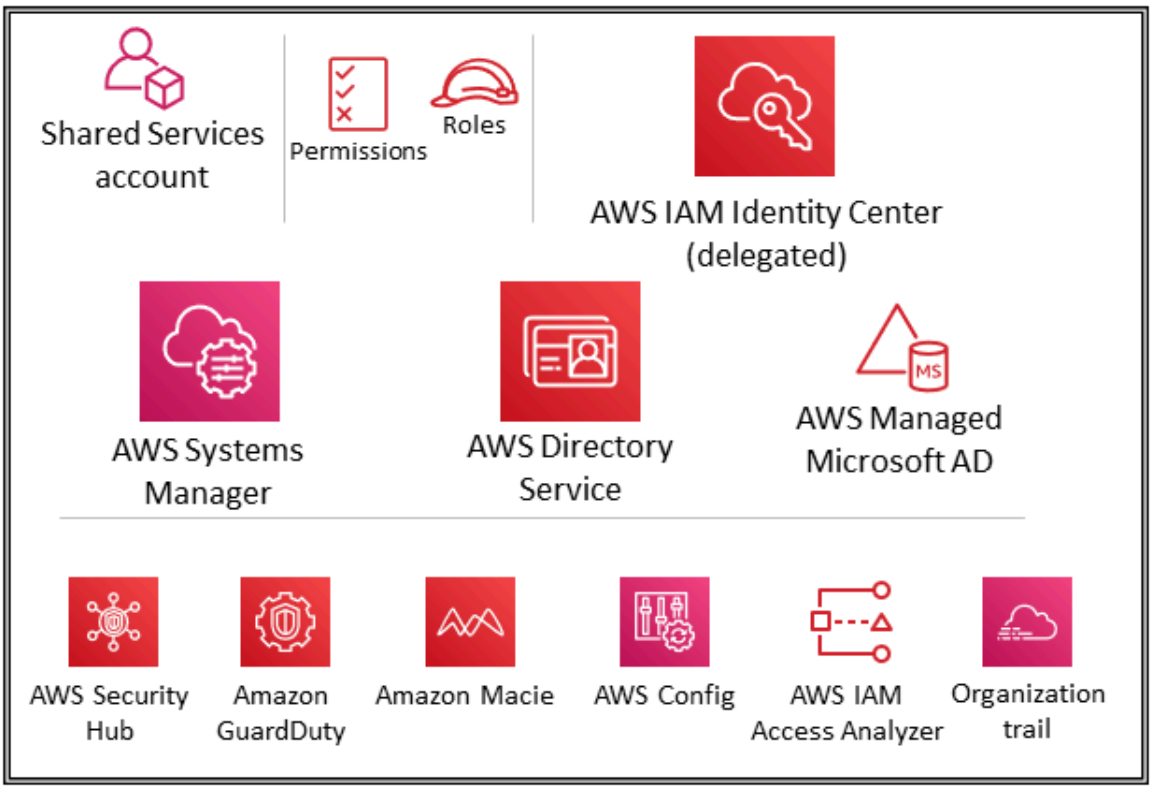
Consideração de design

- Embora a RAM da AWS como serviço seja implantada somente na conta de rede no AWS SRA, ela normalmente seria implantada em mais de uma conta. Por exemplo, você pode centralizar seu gerenciamento de data lake em uma única conta de data lake e depois compartilhar os recursos do catálogo de dados do AWS Lake Formation (bancos de dados e tabelas) com outras contas em sua organização da AWS. Para obter mais informações, consulte a documentação do AWS Lake Formation e a postagem no blog da AWS Compartilhe seus dados com segurança em todas as contas da AWS usando o AWS Lake Formation. Além disso, os administradores de segurança podem usar a RAM da AWS para seguir as melhores práticas ao criar umaCA privada da AWS hierarquia. As CAs podem ser compartilhadas 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.

Infraestrutura OU - Conta de serviços compartilhados

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

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



A conta de Serviços Compartilhados faz parte da UO de Infraestrutura e seu objetivo é dar suporte aos serviços que vários aplicativos e equipes usam para entregar 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 UO de infraestrutura, elas são removidas da conta de Serviços Compartilhados para apoiar a separação de funções. As equipes que gerenciarão esses serviços não precisam de permissões ou acesso às contas da Rede.

AWS Systems Manager

O AWS Systems Manager (que também está incluído na conta de gerenciamento de organizações e na conta do aplicativo) fornece um conjunto de recursos que permitem a visibilidade e o controle de seus recursos da AWS. Um desses recursos, o Systems Manager, é um painel de operações personalizável que fornece informações sobre os recursos da AWS. Você pode sincronizar dados de operações em todas as de sua organização de AWS em todas as de sua organização da AWS, usando o AWS Organizations e Systems Manager. O Systems Manager é implantado na conta do Shared Services por meio da funcionalidade de administrador delegado no AWS Organizations.

O Systems Manager ajuda você a manter a segurança e a conformidade verificando suas instâncias gerenciadas e gerando relatórios (ou tomando medidas corretivas) sobre quaisquer violações de políticas detectadas. Ao combinar o Systems Manager com a implantação apropriada em contas individuais da AWS de membros (por exemplo, a conta do aplicativo), você pode coordenar a coleta de dados de inventário de instâncias e centralizar a automação, como correções e atualizações de segurança.

Microsoft AD gerenciado pela AWS, Microsoft AD

O AWS Directory Service for Microsoft Active Directory, também conhecido como AWS Managed Microsoft AD, permite que suas cargas de trabalho e recursos da AWS. Você pode usar o 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 usar serviços de computação de usuário final (EUC) da AWS, como Amazon WorkSpaces, com Active Usuários e grupos do diretório.

O AWS Managed Microsoft AD ajuda você a estender seu Active Directory existente para a AWS e usar suas credenciais de usuário locais existentes para acessar os recursos da 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 domínio do AWS Managed Microsoft AD.

O AWS Managed Microsoft AD foi criado 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 familiares de administração do Active Directory, como Objetos de Política de Grupo (GPOs), relações de confiança de domínio, políticas de senha refinadas, contas de serviços gerenciados de grupo (GMSAs), 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 diretório AWS Managed Microsoft AD em várias 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.

O 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, o 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 domínio Microsoft AD gerenciados pela AWS a partir de uma autoridade de certificação (CA) do Active Directory Certificate Services (AD CS) baseada na AWS. Ao atuar como cliente, o AWS Managed Microsoft AD oferece suporte a LDAPS nas portas 636 (SSL). Você pode habilitar as comunicações LDAPS do lado do cliente registrando certificados de CA dos emissores de certificados do servidor na AWS e, em seguida, habilitar o LDAPS em seu diretório.

No AWS SRA, o AWS 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 da AWS.

Consideração do design

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

IAM Identity Center

O AWS SRA usa o recurso de administrador delegado suportado pelo IAM Identity Center 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 acessar a conta do Org Management. O IAM Identity Center ainda precisa estar habilitado na conta do Org Management para realizar determinadas tarefas, incluindo o gerenciamento de conjuntos de permissões que são provisionados na conta do Org Management.

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 em que você ativou

o recurso de administrador delegado do IAM Identity Center. No AWS SRA, a conta do Shared Services hospeda o AWS Managed Microsoft AD, de modo que essa conta se torne administradora delegada do IAM Identity Center.

O IAM Identity Center oferece suporte ao registro de uma única conta de membro como administrador delegado ao mesmo tempo. Você pode registrar uma conta de membro somente ao fazer 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.

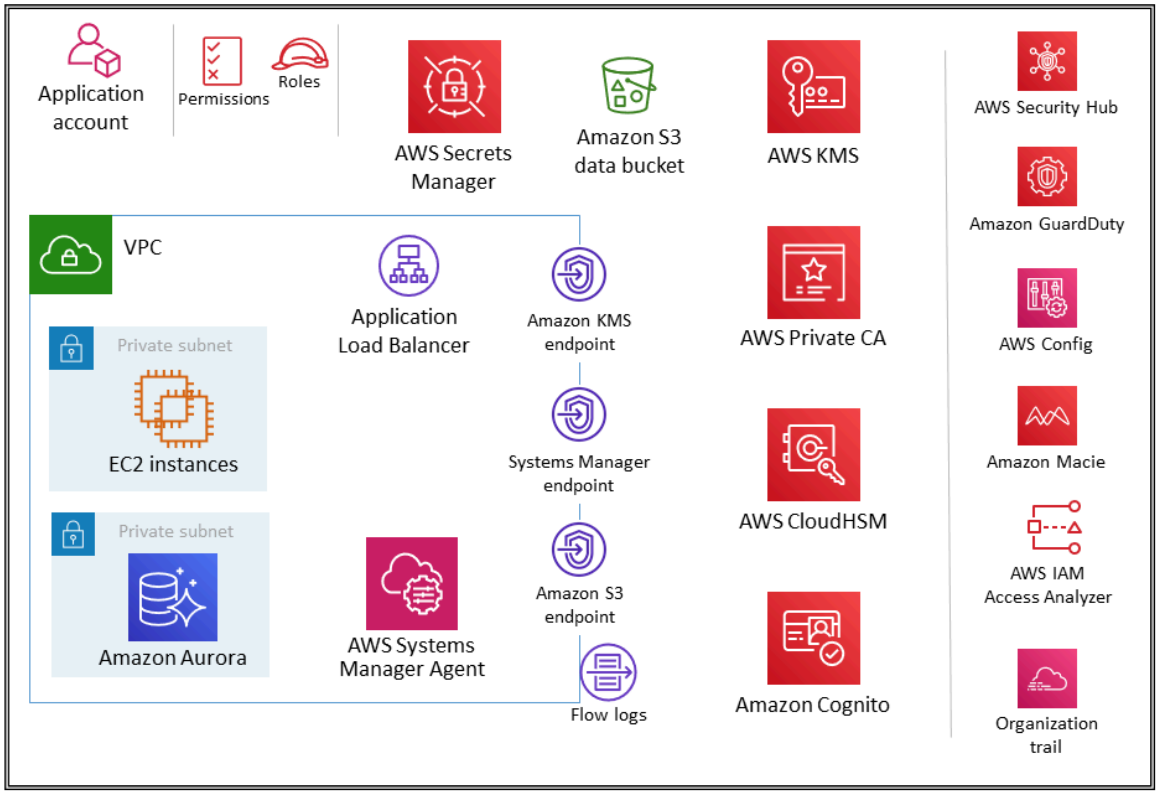
Consideração do design

- 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 a) a conta de membro do administrador delegado do IAM Identity Center, se houver; caso contrário, ele deverá estar na conta de gerenciamento.

Cargas de trabalho OU - Conta de aplicativo

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

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



A conta do aplicativo hospeda a infraestrutura e os serviços primários para executar e manter um aplicativo corporativo. A conta do aplicativo e as cargas de trabalho ou atendem a alguns objetivos primários 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 contas 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. Empregue uma trilha organizacional e implantações locais de serviços de segurança de contas (Amazon GuardDuty, AWS Config, AWS Security Hub, Amazon EventBridge, AWS IAM Access Analyzer), que são configurados e monitorados pela equipe de segurança. Finalmente, você permite que sua empresa defina 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 barreiras de proteção de serviço apropriadas.

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 saída (para necessidades de aplicativos ou necessidades de serviços da AWS). Por padrão, os recursos dentro de uma VPC são roteáveis entre si. Há duas sub-redes privadas: uma para hospedar as instâncias do EC2 (camada de aplicação) e outra para o Amazon Aurora (camada de banco de dados). A segmentação de rede entre diferentes níveis, como a camada do aplicativo e a camada do banco de dados, é realizada por meio de grupos de segurança 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.

Consideração de design

- É possível usar o espelhamento de tráfego para copiar o tráfego de rede de uma elastic network interface de instâncias do EC2. Depois, é possível enviar o tráfego para dispositivos de monitoramento e out-of-band segurança 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 dentro da sua VPC, e o enviará para um único dispositivo de monitoramento. Os registros de fluxo do Amazon VPC não capturam tráfego espelhado; eles geralmente capturam informações somente de cabeçalhos de 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 elastic network interface de instâncias do EC2 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.

VPC endpoints

Os endpoints VPC fornecem outra camada de controle de segurança, bem como escalabilidade e confiabilidade. Use-os para conectar a VPC da aplicação a outros serviços da AWS. (Na conta do aplicativo, o AWS SRA emprega endpoints VPC para AWS KMS, AWS Systems Manager e 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 VPC endpoint para conectar de forma privada a VPC aos serviços da AWS compatíveis e aos serviços do VPC endpoint desenvolvidos pela AWS PrivateLink sem exigir um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na sua VPC não exigem que endereços IP públicos se comuniquem com outros serviços da AWS. O tráfego entre a sua VPC e os outros serviços da AWS não deixa a rede da Amazon.

Outro benefício do uso de endpoints VPC é permitir a configuração de políticas de endpoint. Uma política de VPC endpoint é uma política de recursos do IAM que você anexa a um endpoint quando cria ou

modifica o endpoint. Se você não associar uma política do IAM ao criar um endpoint, a AWS associará uma política do IAM padrão para você que permita o acesso total ao serviço. Uma política de endpoint não substitui políticas 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 a qual os diretores da AWS podem se comunicar com recursos ou serviços.

Amazon EC2

As instâncias do EC2 que compõem nosso aplicativo usam a versão 2 do Instance Metadata Service (IMDSv2). O IMDSv2 adiciona proteções para quatro tipos de vulnerabilidades que poderiam 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 Adicionar defesa profunda contra firewalls abertos, proxies reversos e vulnerabilidades SSRF com melhorias no serviço de metadados de instâncias do EC2.

Use VPCs separados (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 API do Amazon EC2 da VPC sem enviar tráfego pela Internet pública, use a AWS PrivateLink. Restrinja o acesso a suas instâncias usando grupos de segurança. Use Logs de fluxo da VPC para monitorar o tráfego recebido nas instâncias. Use o Gerenciador de sessões do, um recurso do AWS Systems Manager, para acessar suas instâncias remotamente em vez de abrir portas SSH de entrada e chaves SSH. Use volumes separados do Amazon Elastic Block Store (Amazon EBS) para o sistema operacional e seus dados. Você pode configurar sua conta da AWS para impor a criptografia das novas cópias de snapshots e volumes do EBS que criar.

Application Load Balancers

Os Application Load Balancers distribuem o tráfego de entrada de aplicativos em vários destinos, como instâncias do EC2, em várias Zonas de disponibilidade. No AWS SRA, o grupo de destino para o balanceador de carga são as instâncias do EC2 do aplicativo. 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 de front-end e, em seguida, descriptografar solicitações de clientes antes de enviá-las aos destinos.

O AWS Certificate Manager (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 de 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 deCA privada da AWS. No AWS SRA, a CA privada raiz do ACM é hospedada na conta do Security Tooling e pode ser compartilhada com toda a organização da AWS ou com contas específicas da AWS para emitir certificados de entidade final, conforme descrito anteriormente na seção de contas do Security Tooling (p. 41).
- Para certificados públicos, você pode usar o ACM para gerar esses certificados e gerenciá-los, incluindo a rotação automatizada. Como alternativa, você pode gerar seus próprios certificados usando ferramentas SSL/TLS para criar uma solicitação de assinatura de certificado (CSR), obter a assinatura de um CA no CSR para produzir um CA e, depois, importar o CA no ACM ou fazer upload do certificado no IAM para uso com o Application Load Balancer. Se você importar um CA para o ACM, deverá monitorar a data de validade do CA e renová-lo antes que expire.
- Para camadas adicionais de defesa, você pode implantar políticas do AWS WAF para proteger o Application Load Balancer. Ter políticas de ponta, 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 o AWS Managed Rules for AWS WAF.

CA privada da AWS

AWS Private Certificate Authority(CA privada da AWS) é usado na conta do aplicativo para gerar certificados privados a serem usados com um Application Load Balancer. É 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, certificados TLS privados podem fornecer o canal seguro.

No AWS SRA,CA privada da AWS está hospedado na conta Security Tooling e é compartilhado com a conta do aplicativo usando a RAM da AWS. Isso permite que os desenvolvedores em uma conta de aplicativo solicitem um certificado de uma CA privada compartilhada. O compartilhamento de CAs em sua organização ou entre contas da AWS ajuda a reduzir o custo e a complexidade da criação e do gerenciamento de CAs duplicadas em todas as suas 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 verificar automaticamente instâncias do EC2 e imagens de contêiner que residem no Amazon Elastic Container Registry (Amazon ECR) para vulnerabilidades de software e exposição de rede não intencional.

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

O Amazon Inspector nas contas dos membros é gerenciado centralmente pela conta de administrador delegado. No AWS SRA, a conta do Security Tooling é a conta delegada do administrador. A conta de administrador delegado pode gerenciar dados de descobertas 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 de escaneamentos de contas de membros e a revisão dos recursos digitalizados dentro da organização da AWS.

Consideração de design

- Você pode usar o Patch Manager, um recurso do AWS Systems Manager, para acionar patches sob demanda para remediar vulnerabilidades críticas de segurança ou de dia zero do Amazon Inspector. O Patch Manager ajuda você a corrigir essas vulnerabilidades sem ter que esperar pelo cronograma normal de patches. A correção é realizada usando o runbook de automação do Systems Manager. Para obter mais informações, consulte a série de blog em duas partes: Automatize o gerenciamento e a correção de vulnerabilidades na AWS usando o Amazon Inspector e o AWS Systems Manager.

Systems Manager da Amazon

O AWS Systems Manager é um serviço da AWS que você pode usar para exibir dados operacionais de vários serviços da AWS e automatizar tarefas operacionais nos recursos da AWS. 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 nos recursos da AWS.

Além desses recursos gerais de automação, o Systems Manager oferece suporte a vários recursos de segurança preventivos, de detecção e responsivos. O AWS Systems Manager Agent (Agente do SSM) é um software da Amazon que pode ser instalado e configurado em uma instância do EC2, 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 verificando essas instâncias gerenciadas e gerando relatórios (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 hosts bastion ou gerenciar chaves SSH. O AWS SRA usa o Patch Manager, um recurso do Systems Manager, para aplicar patches às instâncias do EC2 para sistemas operacionais e aplicativos.

O AWS SRA também usa a automação, um recurso do Systems Manager, para simplificar tarefas comuns de manutenção e implantação das instâncias do Amazon EC2 e outros recursos da AWS. 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 único clique para simplificar tarefas complexas, como a criação de Amazon Machine Images (AMIs) e a recuperação de instâncias inacessíveis do EC2. Além disso, você pode aprimorar a segurança operacional dando às funções do IAM acesso a runbooks específicos para executar determinadas funções, sem conceder permissões diretamente a essas funções. Por exemplo, se você quiser que uma função do IAM tenha permissões para reiniciar instâncias específicas do EC2 após as atualizações do patch, 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 agente do Systems Manager depende dos metadados da instância do EC2 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 Agent do SSM deve se comunicar com diferentes serviços e recursos da AWS, como mensagens do Amazon EC2, Systems Manager e Amazon S3. Para que essa comunicação ocorra, a sub-rede exige conectividade de saída com a Internet ou provisionamento de endpoints VPC apropriados. O AWS SRA usa endpoints VPC para que o SSM Agent 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 práticas recomendadas para o gerenciamento de recursos em runbooks e compartilhar os runbooks em regiões e grupos da AWS. Você pode também restringir os valores permitidos para 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 organização da AWS. Os casos de uso comuns incluem a capacidade de implementar centralmente a aplicação de patches e atualizações de segurança, corrigir oscilações nas configurações da VPC ou políticas de bucket do S3 e gerenciar instâncias do EC2 em escala. Para obter detalhes da implementação, consulte a documentação do Systems Manager.

Amazon Aurora

No AWS SRA, o Amazon Aurora e o Amazon S3 compõem o nível lógico de dados. O Aurora é um mecanismo de banco de dados relacional gerenciado compatível com o MySQL e o PostgreSQL. Um aplicativo executado nas instâncias do EC2 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.

Consideração de 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 de banco de dados e instâncias de banco de dados do Aurora, use o IAM. Para controlar quais dispositivos e instâncias do EC2 podem abrir conexões para o endpoint do cluster e a porta da instância de banco de dados da instância de banco de dados dos clusters de banco de dados do Aurora em uma VPC, use um grupo de segurança da VPC. Para autenticar logins e permissões para um cluster de banco de dados do Aurora, você pode utilizar a mesma abordagem com uma instância de banco de dados autônoma do MySQL ou do PostgreSQL, ou você pode usar a autenticação de banco de dados do IAM para a edição compatível com o Aurora MySQL. Com essa última abordagem, é possível autenticar 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 muitos aplicativos criados na 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, as palestras técnicas on-line e informações 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 gerenciamento de chaves, em que a chave KMS reside na mesma conta da AWS que o recurso a ser criptografado. Por esse motivo, o AWS KMS é usado na conta do aplicativo, além de ser incluído na conta do Security Tooling. Na conta do aplicativo, o AWS KMS é usado para gerenciar chaves específicas dos recursos do aplicativo. Você pode implementar uma separação de tarefas usando as principais políticas para conceder permissões de uso de chaves às funções locais do aplicativo e restringir as permissões de gerenciamento e monitoramento aos seus principais guardiões.

Consideração de design

- Em um modelo distribuído, a responsabilidade de gerenciamento de chaves do AWS KMS é da equipe de aplicativos. No entanto, sua equipe central de segurança pode ser responsável pela governança e monitoramento de eventos criptográficos importantes, como os seguintes:
  - O material da chave importada em uma chave do KMS está próximo da data de validade.
  - Uma chave do KMS com exclusão pendente ainda está sendo usada.
  - O material de chave em uma chave do KMS foi alternado automaticamente.
  - Uma chave do KMS foi excluída.
  - Há uma alta taxa de falha na decodificação.

AWS CloudHSM

O AWS CloudHSM oferece módulos de segurança de hardware gerenciados (HSMs) na nuvem da AWS. Ele permite que você gere e use suas próprias chaves de criptografia na AWS usando HSMs validados pelo FIPS 140-2 nível 3 aos quais você controla o acesso. Você pode usar o CloudHSM para transferir o processamento SSL/TLS para seus servidores web. Isso reduz a carga sobre o servidor web e fornece segurança extra ao armazenar a chave privada do servidor web no CloudHSM. Da mesma forma, você pode implantar um HSM do CloudHSM na VPC de entrada na conta de rede para armazenar suas chaves

privadas e assinar solicitações de certificado se precisar atuar como uma autoridade de certificação emissora.

Consideração de design

- Se você tiver uma exigência rígida para o FIPS 140-2 nível 3, você também pode optar por configurar o AWS KMS para usar o cluster do CloudHSM como um armazenamento de chaves personalizado em vez de usar o armazenamento de chaves nativo do KMS. Ao fazer isso, você se beneficia da integração entre o AWS KMS e os serviços da AWS que criptografam seus dados, além de ser responsável pelos HSMs que protegem suas chaves do KMS. Isso combina HSMs de locatário único sob seu controle com a facilidade de uso e integração do AWS KMS. Para gerenciar sua infraestrutura do CloudHSM, você precisa empregar uma infraestrutura de chave pública (PKI) e ter uma equipe com experiência no gerenciamento de HSMs.

AWS Secrets Manager

O AWS Secrets Manager ajuda você a proteger as credenciais (segredos) de que você precisa para acessar seus aplicativos, serviços e recursos de TI. O serviço permite alternar, gerenciar e recuperar com eficiência credenciais de banco de dados, chaves de API e outros segredos durante seu ciclo de vida. Você pode substituir credenciais codificadas, incluindo o, por uma chamada de API ao Secrets Manager para recuperar o segredo por programação. 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 com nome e referência apropriados 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 refinadas do IAM e políticas baseadas em recursos. Você pode ajudar a proteger segredos criptografando-os com chaves de criptografia que você gerencia usando o AWS KMS. O Secrets Manager também se integra aos serviços de registro e monitoramento da AWS para auditoria centralizada.

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

Como prática recomendada, você pode monitorar seus segredos para registrar quaisquer alterações neles. Isso ajuda a garantir que qualquer alteração ou uso inesperado possa ser investigado. 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 e AWS Config. 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 as APIs do Secrets Manager. Além disso, CloudTrail captura outros eventos relacionados (não relacionados à API) que podem causar impacto na segurança ou na compatibilidade da sua conta da AWS ou podem ajudar você a solucionar problemas operacionais. Isso inclui certos eventos de rotação de segredos e exclusão de versões secretas. O AWS Config pode fornecer controles de detetive rastreando e monitorando alterações em segredos no Secrets Manager. Essas mudanças incluem a descrição de um segredo, a configuração de rotação, as tags e o relacionamento com outras fontes da AWS, como a chave de criptografia KMS ou as funções do AWS Lambda usadas para rotação secreta. Você também pode configurar a Amazon EventBridge, que recebe notificações de alterações de configuração e conformidade do AWS Config, para encaminhar eventos secretos específicos para ações de notificação ou remediação.

No AWS SRA, o Secrets Manager está localizado na conta do aplicativo para dar suporte a casos de uso de aplicativos locais e gerenciar segredos próximos ao seu uso. Aqui, um perfil de instância é anexado às instâncias do EC2 na conta do aplicativo. Em seguida, segredos separados podem ser configurados no

Secrets Manager para permitir que o perfil da instância recupere segredos — por exemplo, para ingressar no domínio apropriado do Active Directory ou LDAP e acessar o banco de dados do Aurora.

Consideração de 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 em que 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 de usuários, login e controle de acesso aos seus aplicativos web e móveis de forma rápida e eficiente. O Amazon Cognito se expande 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 identidade. Os grupos de usuários são diretórios de usuários que fornecem opções de cadastro e login para os usuários do aplicativo. Os grupos de identidade permitem que você conceda aos 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 oferece uma interface de usuário integrada e personalizável para login e cadastro de usuários. Você pode usar o Android, o iOS e JavaScript os SDKs do Amazon Cognito para adicionar páginas de cadastro e login de usuários aos seus aplicativos. O Amazon Cognito Sync é um serviço da AWS e uma biblioteca de clientes que permite a sincronização dos dados de usuários relacionados a aplicações entre dispositivos.

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

Considerações sobre design

- Você pode criar uma função do AWS Lambda e, depois, acionar essa função durante as operações do grupo de usuários, como cadastro do usuário, confirmação e login (autenticação) com um acionador do AWS 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 pequenas aplicações multilocatário. Um caso de uso comum de projeto de vários locatários é executar workloads para oferecer 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 locatários e o volume esperado se alinham com as cotas de serviço relacionadas do Amazon Cognito. Essas cotas são compartilhadas entre todos os locatários da aplicação.

Defesa em camadas

A conta do aplicativo oferece uma oportunidade de ilustrar os princípios de defesa em camadas que a AWS habilita. Considere a segurança das instâncias do EC2 que compõem o núcleo de um aplicativo

de exemplo simples representado no AWS SRA e você poderá ver como os serviços da AWS funcionam juntos em uma defesa em camadas. Essa abordagem se alinha à visão estrutural dos serviços de segurança da AWS, conforme descrito na seção Aplicar serviços de segurança em toda a sua organização da AWS (p. 17), anteriormente neste guia.

- A camada mais interna são as instâncias do EC2. Conforme mencionado anteriormente, as instâncias do EC2 incluem muitos recursos de segurança nativos, por padrão ou como opções. Os exemplos incluem o IMDSv2, o sistema Nitro e a criptografia de armazenamento do Amazon EBS.
- A segunda camada de proteção se concentra no sistema operacional e no software executado nas instâncias do EC2. Serviços como o Amazon Inspector e o AWS Systems Manager permitem monitorar, relatar e tomar medidas corretivas nessas configurações. O 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 quaisquer ações corretivas que você especificar.
- As instâncias e o software executado nessas instâncias estão em sua infraestrutura de rede da AWS. Além de usar os recursos de segurança do Amazon VPC, o AWS SRA também usa endpoints VPC para fornecer conectividade privada entre a VPC e os serviços da AWS suportados e para fornecer um mecanismo para colocar as políticas de acesso nos limites da rede.
- A atividade e a configuração das instâncias, software, rede e funções e recursos do IAM do EC2 são monitoradas ainda mais por serviços focados em contas da AWS, como AWS Security Hub GuardDuty, Amazon CloudTrail, AWS, AWS Config, AWS IAM Access Analyzer e Amazon Macie.
- Por fim, além da conta do aplicativo, a RAM da AWS ajuda a controlar quais recursos são compartilhados com outras contas, e as políticas de controle de serviços do IAM ajudam você a aplicar permissões consistentes em toda a organização da AWS.

Recursos do IAM

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) 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 organização da AWS, das contas da AWS e dos serviços da AWS. Você não pode implantar nenhum serviço da AWS sem criar entidades do IAM e conceder permissões primeiro. 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 obter as melhores práticas do IAM, consulte as melhores práticas de segurança no IAM na documentação da AWS, artigos do IAM no blog de segurança da AWS e apresentações do AWS re:Invent.
- O pilar de segurança do AWS Well-Architected descreve as principais etapas do processo de gerenciamento de permissões: definir barreiras de proteção de permissões, conceder acesso mínimo de privilégios, analisar o acesso público e entre contas, compartilhar recursos com segurança, reduzir as permissões continuamente e estabelecer um processo de acesso emergencial.
- A tabela a seguir e suas notas anexas fornecem uma visão geral de alto nível das orientações recomendadas sobre os tipos de políticas de permissão do IAM disponíveis e como usá-las em sua arquitetura de segurança. Para saber mais, veja o vídeo 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 serviço (SCPs)	Restrict	Equipe central, como plataforma ou equipe de segurança [1]	Guarções e governança	Organização, OU, conta	Todos os diretores em Organização, UO e contas	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 restrições	Equipe central, como equipe de plataforma, segurança ou IAM [1]	Permissões para funções (básicas) que não sejam de automação de carga de trabalho [3]	Conta única [4]	Diretores usados pela automação em uma conta de membro	Contas-membro

Políticas humanas básicas (as funções do IAM que concedem aos usuários permissões para realizar seu trabalho)	Conceder e restrições	Equipe central, como equipe de plataforma, segurança ou IAM [1]	Permissões para funções humanas [5]	Conta única [4]	Diretores federados [5] e usuários do IAM [6]	Contas-membro
Limites de permissões (permissões máximas que um desenvolvedor capacitado pode atribuir a outro diretor)	Restrict	Equipe central, como equipe de plataforma, segurança ou IAM [1]	Barras de proteção para funções de aplicativos (devem ser aplicadas)	Conta única [4]	Funções individuais para um aplicativo ou carga de trabalho nessa conta [7]	Contas-membro
Políticas de função de máquina para aplicativos (função associada à infraestrutura implantada por desenvolvedores)	Conceder e restrições	Delegado aos desenvolvedores [8]	Permissão para o aplicativo ou carga de trabalho [9]	Conta única	Um principal nesta conta	Contas-membro
Políticas de recursos	Conceder e restrições	Delegado aos desenvolvedores [8,10]	Permissões para recursos	Conta única	Um principal em uma conta [11]	Contas-membro

Notas da tabela:

1. As empresas têm muitas equipes centralizadas (como plataformas de 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 funções mais eficaz para sua empresa.
2. Para usar SCPs, você deve habilitar todos os recursos dentro do 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, regras do AWS Lambda e do AWS Config) e outras permissões. Essa configuração geralmente é entregue quando a conta é provisionada.
4. Embora eles pertençam a um recurso (como uma função ou uma política) em uma única conta, eles podem ser replicados ou implantados em várias contas usando a 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 de contas).

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 sobre 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, impõem a anexação do limite de permissões.
8. Isso pressupõe que barreiras 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 permissões do próprio desenvolvedor do aplicativo.
10. Além das permissões de contas locais, uma equipe centralizada (como a equipe da plataforma de 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 diretor em qualquer conta para permitir ou negar acesso a seus recursos. Pode até mesmo se referir a diretores anônimos para permitir o acesso público.

Garantir que as identidades do IAM tenham somente 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 privilégios mínimos 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 de proteção e limites de permissões específicos.
- Implemente o mínimo de privilégios por meio de um processo continuamente iterativo. Este não é um exercício único.
- Use SCPs para reduzir o risco acionável. Eles se destinam a ser grades de proteção amplas, não controles direcionados de forma restrita.
- Use limites de permissões para delegar a administração do IAM de forma mais segura.
  - Certifique-se de que os administradores delegados associem a política de limites apropriada do IAM 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 CloudTrail, o AWS, o AWS IAM Access Analyzer e as ferramentas relacionadas para analisar regularmente o histórico de uso 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, revisar e aprovar rapidamente as exceções da política do IAM com base nas solicitações.

Repositório de código para exemplos de SRA da AWS

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) 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 AWS Professional Services 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 configurações de serviços e as implantações de recursos da AWS são deliberadamente muito restritivas. Talvez seja necessário modificar e adaptar essas soluções para atender às suas necessidades ambientais e de segurança.

Os exemplos neste repositório foram implantados e testados em um ambiente de torre de controle da AWS usando a AWS CloudFormation e a solução Customizations for AWS Control Tower (cFCT). A solução cFCT ajuda os clientes a configurar rapidamente um ambiente seguro e com várias contas da AWS com base nas melhores práticas da AWS. 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. A 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 arquivo README.md com detalhes.

- A solução CloudTrail Organization cria uma trilha organizacional dentro da conta do Org Management. Essa trilha é criptografada com uma chave gerenciada pelo cliente criada na conta do Security Tooling e entrega registros em um bucket do S3 na conta Log Archive. Opcionalmente, eventos de dados podem ser habilitados para funções do Amazon S3 e do AWS Lambda. Uma trilha organizacional registra eventos de todas as contas da AWS na organização da AWS, ao mesmo tempo em que impede 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 future da organização da AWS. 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 Organization configura o AWS Security Hub delegando a administração à conta do Security Tooling. Ele configura o Security Hub na conta do Security Tooling para todas as contas existentes e future da organização da 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 Security Hub na conta do Security Tooling fornece uma visão entre contas da conformidade com os padrões de segurança e das descobertas dos serviços da AWS e de integrações de terceiros com parceiros da AWS.
- A solução Firewall Manager configura as políticas de segurança do AWS Firewall Manager delegando a administração à conta do Security Tooling e configurando o Firewall Manager com uma política de grupo

de segurança e várias políticas do AWS WAF. A política do grupo de segurança exige um grupo de segurança máximo permitido dentro de 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 future da organização da AWS. Além disso, o Macie está 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 agregador do AWS Config delegando a administração à conta do Security Tooling. Em seguida, a solução configura um agregador do AWS Config na conta do Security Tooling para todas as contas existentes e future na organização da AWS.
  - A solução Conformance Pack Organization Rules implanta as regras do AWS Config delegando a administração à conta do Security Tooling. Em seguida, ele cria um pacote de conformidade organizacional dentro da conta do administrador delegado para todas as contas existentes e future na organização da AWS. A solução está configurada para implantar o modelo de pacote de amostra de pacote de conformidade de melhores práticas operacionais para criptografia e gerenciamento de chaves.
  - A solução de conta de gerenciamento da AWS Config Control Tower habilita o AWS Config na conta de gerenciamento da AWS Control Tower e atualiza o agregador AWS Config dentro da conta do Security Tooling adequadamente. A solução usa o CloudFormation modelo AWS Control Tower para habilitar o AWS Config como referência para garantir a consistência com as outras contas na organização da AWS.
- IAM
  - A solução Access Analyzer habilita o AWS IAM Access Analyzer delegando a administração à conta do Security Tooling. Em seguida, ele configura um Analisador de Acesso em nível organizacional dentro da conta do Security Tooling para todas as contas existentes e future na organização da AWS. A solução também implanta o Access Analyzer em todas as contas e regiões dos membros para apoiar a análise de permissões em nível de conta.
  - A solução IAM Password Policy atualiza a política de senha da conta da AWS em todas as contas em uma organização da AWS. 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 padrão do EBS do EC2 permite a criptografia padrão do Amazon EBS em nível de conta em cada conta da AWS e região da AWS na organização da AWS. Ele impõe a criptografia dos novos volumes e snapshots do EBS que você cria. Por exemplo, o Amazon EBS criptografará os volumes do EBS que são criados quando você executar uma instância e os snapshots que copiar a partir de um snapshot não criptografado.
- A solução S3 Block Account Public Account permite configurações em nível de conta do Amazon S3 em cada conta da AWS na organização da 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 Bloqueio de acesso público do Amazon S3 substituem essas políticas e permissões, de maneira que seja possível limitar o acesso público a esses recursos.

Agradecimentos

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

Autores primários

- Avik Mukherjee, consultor sênior da AWS
- Andy Wickersham, consultor sênior da AWS
- Neal Rothleder, consultor principal da AWS
- Paul Grassi, consultor principal da AWS

Colaboradores

- Scott Conklin, consultor sênior da AWS
- Josh Du Lac, principal arquiteto de soluções da AWS
- Michael Haken, principal tecnólogo da AWS
- Jorg Huser, consultor principal da AWS
- Mehial Mendrin, consultor sênior da AWS
- Eric Rose, consultor principal da AWS
- Ilya Epshteyn, gerente sênior de soluções de identidade
- Handan Selamoglu, redator técnico sênior da AWS

Apêndice: Serviços de segurança, identidade e conformidade da AWS

Influencie o future da Arquitetura de Referência deAWS Segurança (AWSSRA) respondendo a uma breve pesquisa.

Para uma introdução ou uma atualização, consulte Segurança, identidade e conformidade na AWS no site da AWS 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 — A 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 machine learning.
- AWS KMS — Crie e controle as chaves usadas para criptografar seus dados.
- AWS CloudHSM — Gerencie seus módulos de segurança de hardware (HSMs) na nuvem da AWS.
- AWS Certificate Manager: provisionar, gerenciar e implantar os certificados SSL/TLS para uso com os serviços da AWS.
- AWS Secrets Manager: alterne, gerencie e recupere credenciais de banco de dados, chaves de API e outros segredos durante seu ciclo de vida.

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

- IAM — Controle com segurança o acesso aos serviços e recursos da AWS.
- IAM Identity Center — gerencie centralmente o acesso por SSO a várias contas e aplicativos de negócios da AWS.
- Amazon Cognito — Adicione inscrição, login e controle de acesso de usuários aos seus aplicativos web e móveis.
- AWS Directory Service: use o Microsoft Active Directory gerenciado na Nuvem AWS.
- AWS Resource Access Manager — compartilhe recursos da AWS de forma simples e segura.
- AWS Organizations — Implemente o gerenciamento baseado em políticas para várias contas da AWS.

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

- AWS Shield — Proteja seus aplicativos web que são executados na AWS com proteção gerenciada contra DDoS.
- AWS WAF — Proteja seus aplicativos da web contra explorações comuns da web e garanta disponibilidade e segurança.

- AWS Firewall Manager — configure e gerencie as regras do AWS WAF em todas as contas e aplicativos da AWS a partir de um local central.
- AWS Systems Manager — configure e gerencie o Amazon EC2 e sistemas locais para aplicar patches de sistema operacional, criar imagens de sistema seguras e configurar sistemas operacionais seguros.
- Amazon VPC: provisiona uma seção logicamente isolada da AWS onde é possível executar recursos da AWS em uma rede virtual que você define.
- AWS Network Firewall — Implemente proteções de rede essenciais para suas VPCs.
- Firewall DNS Firewall do Amazon Route 53: proteja suas solicitações DNS de saída de suas VPCs.

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

- AWS Security Hub — Visualize e gerencie alertas de segurança e automatize as verificações de conformidade a partir de um local central.
- Amazon GuardDuty — Proteja suas contas e cargas de trabalho da AWS 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 implantados na AWS.
- AWS Config — registre e avalie as configurações de seus recursos da AWS 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 em um estado de boas condições.
- AWS CloudTrail — Acompanhe a atividade do usuário e o uso da API para permitir a governança e a auditoria operacional e de risco de sua 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 — A AWS oferece uma visão abrangente do seu status de conformidade e monitora continuamente seu ambiente usando verificações de conformidade automatizadas com base nas melhores práticas da AWS e nos padrões do setor que sua empresa segue.

- AWS Artifact — Use um portal de autoatendimento gratuito para obter acesso sob demanda aos relatórios de segurança e conformidade da AWS e selecionar contratos on-line.
- AWS Audit Manager: audite continuamente o uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Histórico do documentos

A tabela a seguir descreve alterações significativas neste guia. Se quiser ser notificado sobre future atualizações, você pode assinar um feed RSS.

Alteração	Descrição	Data
Pesquisa (p. 73)	Adicionamos 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 (p. 73)	Na seção Arquitetura de referência deAWS segurança, foi adicionado um arquivo de download que fornece os diagramas de arquitetura desse guia em PowerPoint formato editável.	17 de novembro de 2022
Atualizações na seção Fundamentos de segurança (p. 73)	Na seção Fundamentos de segurança, atualizei as informações sobre os pilares e os princípios de design de segurança da Well-Architected.	27 de setembro de 2022
Principais adições e atualizações (p. 73)	• Foram adicionadas informações sobre como usar o AWS SRA e as principais diretrizes de implementação. • Foi adicionada orientação arquitetônica para serviços adicionais da AWS, como AWS Artifact, Amazon Inspector, AWS RAM, Amazon Route 53, AWS Control Tower, AWS Audit Manager, AWS Directory Service, Amazon Cognito e Network Access Analyzer. • Diretrizes atuais atualizadas para refletir os novos recursos de serviços e as melhores práticas da AWS.	25 de julho de 2022
— (p. 73)	Publicação inicial. Essa versão não inclui váriosAWS serviços (comoAWS Directory Service Amazon Cognito eAWS Audit Manager), que planejamos adicionar em versões future.AWS Resource Access Manager	23 de junho de 2021

AWSGlossário de orientação prescritiva

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

Termos de segurança

controle de acesso baseado em atributos (ABAC)

: A prática de criar permissões refinadas com base nos atributos do usuário, como departamento, função e nome da equipe. Para obter mais informações, consulte ABACAWS na documentaçãoAWS Identity and Access Management (IAM).

criptografia assimétrica

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

gráfico de comportamento

: Uma visão unificada e interativa do comportamento e das interações dos recursos ao longo do tempo. Você pode usar um gráfico de comportamento com o Amazon Detective para examinar tentativas fracassadas de login, chamadas de API suspeitas e ações semelhantes. Para obter mais informações, consulte Dados em um gráfico de comportamento na documentação do Detective.

criptografia no lado do cliente

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

pacote de conformidade do

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

dados em repouso

: Dados que estão estacionários em sua rede, como dados armazenados.

classificação de dados

: Um processo para identificar e categorizar os dados em sua rede com base em sua criticidade e sensibilidade. É um componente essencial de qualquer estratégia de gerenciamento de risco de segurança cibernética, pois ajuda a determinar os controles de proteção e retenção apropriados para os dados. A classificação de dados é um componente do pilar de segurança noAWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

dados em trânsito

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

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente colocados em uma rede de computadores para proteger a confidencialidade, integridade e disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégiaAWS, você adiciona vários controles em diferentes camadas daAWS Organizations estrutura para ajudar a proteger os recursos.

administrador delegado

EmAWS Organizations, um serviço compatível pode registrar uma conta deAWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta é chamada de administrador delegado desse serviço. Para obter mais informações e uma lista de serviços compatíveis, consulte Serviços com os quais funcionamAWS Organizations naAWS Organizations documentação.

controle de detetive

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 ignoraram os controles preventivos em vigor. Para obter mais informações, consulte Controles de Detective em Implementando controles de segurança emAWS.

chave de criptografia

Uma sequência criptográfica de bits aleatórios gerada por um algoritmo de criptografia. As teclas podem variar em comprimento e cada tecla foi projetada para ser imprevisível e exclusiva.

serviço de endpoint

Um serviço que você pode hospedar em uma virtual private cloud (VPC) para compartilhar com outros usuários. Você pode criar um serviço de endpoint comAWS PrivateLink e conceder permissões a outros diretoresContas da AWS ou a diretores do IAM. Essas contas ou Entidades principais do 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 da Amazon VPC.

criptografia de envelope

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

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. Você pode 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.

corrimão

Uma regra de alto nível que ajuda a controlar recursos, políticas e conformidade em todas as unidades organizacionais (OUs). As barreiras preventivas impõem políticas para garantir o alinhamento aos padrões de conformidade. Eles são implementados usando políticas de controle de serviços e limites de permissões do IAM. As grades de proteção de Detective detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usandoAWS Config,AWS Security Hub, Amazon GuardDutyAWS Trusted Advisor, Amazon Inspector eAWS Lambda verificações personalizadas.

política do baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões noNuvem AWS ambiente.

VPC de entrada (entrada)

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

inspeção VPC

Em uma arquitetura deAWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (iguais ou diferentesRegiões da AWS), a Internet e redes locais. A arquiteturaAWS de referência de segurança recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

privilégio mínimo

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

conta-membro

TudoContas da AWS exceto a conta de gerenciamento que faz parte de uma organização emAWS Organizations. Uma conta da só pode ser membro de uma organização de cada vez.

trilha organizacional

Uma trilha criada porAWS CloudTrail that registra todos os eventos de todosContas da AWS em uma organização emAWS Organizations. Essa trilha é criada em cada umConta da AWS que faz parte da organização e acompanha a atividade em cada conta. Para obter mais informações, consulte Criar uma trilha para uma organização na CloudTrail documentação.

VPC de saída (saída)

Em uma arquitetura deAWS várias contas, uma VPC que manipula conexões de rede que são iniciadas de dentro de um aplicativo. A arquiteturaAWS de referência de segurança recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

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 suporta todos os buckets S3Regiões da AWS, criptografia do lado do servidor comAWS KMS (SSE-KMS) eDELETE solicitações dinâmicasPUT e para o bucket S3.

identidade de 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 princípio 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 CloudFront distribuição específica. Veja também OAC (p. 76), que fornece um controle de acesso mais granular e aprimorado.

limite de permissões

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

política

Um objeto que pode definir permissões (consultepolítica do baseada em identidade (p. 75)), especificar condições de acesso (consultepolítica baseada em recursos (p. 77)) ou definir as

permissões máximas para todas as contas em uma organização emAWS Organizations (consulte a política de controle de serviços (p. 77)).

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 Implementação de controles de segurança emAWS.

principal

Entidade na AWS que pode executar ações e acessar recursos. Essa entidade normalmente é um usuário raiz de umaConta da AWS função do IAM ou de um usuário. Para obter mais informações, consulte os termos e conceitos do Principal in Roles na documentação do IAM.

política baseada em recursos

Uma política anexada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais diretores têm acesso autorizado, ações suportadas e quaisquer outras condições que devem ser atendidas.

controle responsivo

Um controle de segurança projetado para impulsionar a remediação de eventos adversos ou desvios de sua linha de base de segurança. Para obter mais informações, consulte Controles responsivos em Implementação de controles de segurança emAWS.

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite a autenticação única (SSO) federada, para que os usuários possam fazer login noAWS Management Console ou chamar as operações deAWS API da 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.

controle de segurança

Uma barreira técnica ou administrativa que impede, detecta ou reduz a capacidade de um agente ameaçador de explorar uma vulnerabilidade de segurança. Existem três tipos principais de controles de segurança: preventivo (p. 77), detetive (p. 75) e responsivo (p. 77).

fortalecimento da segurança

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

sistema de gerenciamento de informações e eventos 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.

criptografia do lado do servidor

Criptografia de dados em seu destino, pelaAWS service (Serviço da AWS) pessoa que os recebe.

política de controle de serviço (SCP)

Uma política que fornece controle centralizado sobre as permissões para todas as contas em uma organização emAWS Organizations. Os SCPs definem barreiras ou estabelecem limites para 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 naAWS Organizations documentação.

Modelo de responsabilidade compartilhada

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

criptografia simétrica

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

acesso confiável

Conceder permissões a um serviço que você especificar para executar tarefas em sua organização emAWS Organizations e suas contas em seu nome. O serviço confiável cria uma função vinculada ao serviço em cada conta, quando essa função é necessária, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte UsoAWS Organizations com outrosAWS serviços naAWS Organizations documentação.

carga de trabalho

Uma coleção de códigos e recursos que fornece valor comercial, como um aplicativo ou um processo de back-end voltado para o cliente.

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.