AWS Guia de decisão

Escolhendo serviços de AWS segurança, identidade e governança

Escolhendo serviços de AWS segurança, identidade e governança: AWS Guia de decisão

Table of Contents

Escolhendo serviços de AWS segurança, identidade e governança

Dando o primeiro passo

Hora de ler	27 minutos	
Finalidade	Ajudar você a determinar quais serviços de AWS segurança , identidade e governança são mais adequados para sua organização.	
Última atualização	30 de dezembro de 2024	
Serviços cobertos	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS Private CA • AWS RAM • AWS Secrets Manager • AWS Security Hub • Amazon Security Lake • AWS Resposta a incidentes de segurança • AWS Shield • AWS WAF

Introdução

Segurança, identidade e governança na nuvem são componentes importantes para você alcançar e manter a integridade e a segurança de seus dados e serviços. Isso é especialmente relevante

à medida que mais empresas migram para provedores de nuvem, como a Amazon Web Services (AWS).

Este guia ajuda você a selecionar os serviços e ferramentas de AWS segurança, identidade e governança mais adequados às suas necessidades e à sua organização.

Primeiro, vamos explorar o que queremos dizer com segurança, identidade e governança:

- A segurança na nuvem se refere ao uso de medidas e práticas para proteger os ativos digitais contra ameaças. Isso inclui a segurança física dos data centers e as medidas de segurança cibernética para se proteger contra ameaças on-line. AWS prioriza a segurança por meio de armazenamento de dados criptografados, segurança de rede e monitoramento contínuo de possíveis ameaças.
- Os serviços de identidade ajudam você a gerenciar com segurança identidades, recursos e permissões de forma escalável. AWS fornece serviços de identidade projetados para a força de trabalho e aplicativos voltados para o cliente, além de gerenciar o acesso às suas cargas de trabalho e aplicativos.
- A governança da nuvem é um conjunto de regras, processos e relatórios que orientam sua organização a seguir as melhores práticas. Você pode estabelecer a governança da nuvem em todos AWS os seus recursos, usar as melhores práticas e padrões integrados e automatizar os processos de conformidade e auditoria. A conformidade na nuvem se refere à adesão às leis e regulamentações que regem a privacidade e a proteção de dados. AWS Os Programas de Conformidade fornecem informações sobre as certificações, regulamentações e estruturas que se AWS alinham com o.

Este vídeo one-and-a-half minucioso resume como AWS criar uma segurança forte em nossa essência.

AWS Entenda os serviços de segurança, identidade e governança

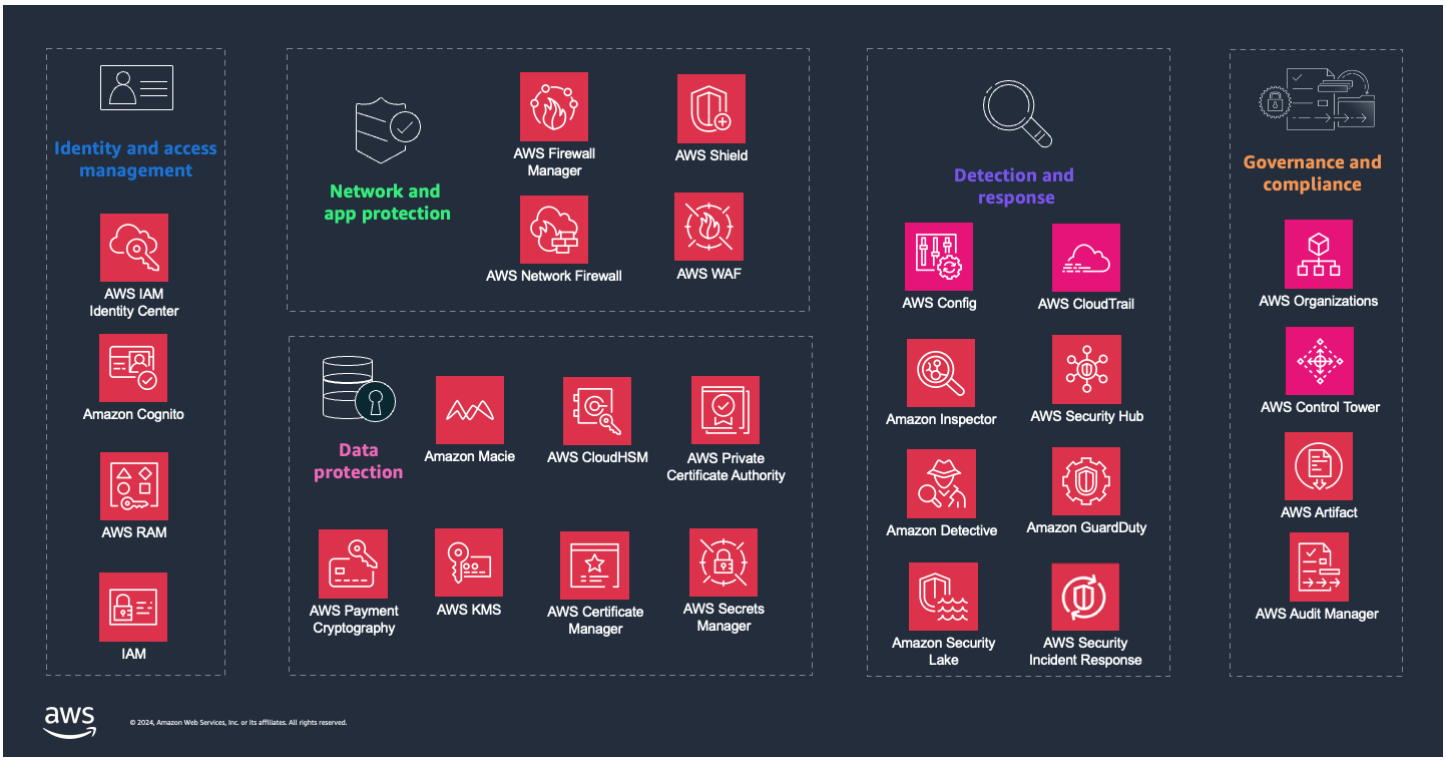
Segurança e conformidade são responsabilidades compartilhadas

Antes de escolher seus serviços de AWS segurança, identidade e governança, é importante que você entenda que segurança e conformidade são responsabilidades compartilhadas entre você AWS e.

A natureza dessa responsabilidade compartilhada ajuda a aliviar sua carga operacional e fornece flexibilidade e controle sobre sua implantação. Essa diferenciação de responsabilidade é comumente chamada de segurança “da” nuvem e segurança “na” nuvem.

Com a compreensão desse modelo, você pode entender a variedade de opções disponíveis e como as opções aplicáveis Serviços da AWS se encaixam.

Você pode combinar AWS ferramentas e serviços para ajudar a proteger suas cargas de trabalho



Conforme mostrado no diagrama anterior, AWS oferece ferramentas e serviços em cinco domínios para ajudá-lo a obter e manter segurança, gerenciamento de identidade e governança robustos na nuvem. Você pode usar Serviços da AWS esses cinco domínios para ajudá-lo a fazer o seguinte:

- Crie uma abordagem em várias camadas para proteger seus dados e ambientes
- Fortaleça sua infraestrutura de nuvem contra ameaças em evolução
- Aderir a padrões regulatórios rígidos

Para saber mais sobre AWS segurança, incluindo a documentação de segurança Serviços da AWS, consulte a Documentação AWS de segurança.

Nas seções a seguir, examinaremos cada domínio mais detalhadamente.

AWS Entenda os serviços de gerenciamento de identidade e acesso

No centro da AWS segurança está o princípio do menor privilégio: indivíduos e serviços têm apenas o acesso de que precisam. AWS IAM Identity Centeré o recomendado AWS service (Serviço da AWS) para gerenciar o acesso do usuário aos AWS recursos. Você pode usar esse serviço para gerenciar o acesso às suas contas e permissões dentro dessas contas, incluindo identidades de provedores de identidade externos.

A tabela a seguir resume as ofertas de gerenciamento de identidade e acesso discutidas neste guia:

AWS IAM Identity Center

> AWS IAM Identity Centerajuda você a conectar sua fonte de identidades ou criar usuários. Você pode gerenciar centralmente o acesso da força de trabalho a vários aplicativos Contas da AWS .

Amazon Cognito

> O Amazon Cognito fornece uma ferramenta de identidade para aplicativos web e móveis para autenticar e autorizar usuários a partir do diretório de usuários incorporado, do seu diretório corporativo e dos provedores de identidade do consumidor.

AWS RAM

> AWS RAMajuda você a compartilhar com segurança seus recursos dentro de sua organização e com funções e usuários do IAM. Contas da AWS

IAM

> O IAM permite um controle seguro e refinado sobre o acesso aos AWS recursos da carga de trabalho.

Entenda os serviços de proteção de AWS dados

A proteção de dados é vital na nuvem e AWS fornece serviços que ajudam você a proteger seus dados, contas e cargas de trabalho. Por exemplo, criptografar seus dados em trânsito e em repouso ajuda a protegê-los da exposição. Com AWS Key Management Service(AWS KMS) e AWS CloudHSMvocê pode criar e controlar as chaves criptográficas que você usa para proteger seus dados.

A tabela a seguir resume as ofertas de proteção de dados discutidas neste guia:

Amazon Macie

O Amazon Macie descobre dados confidenciais usando aprendizado de máquina e correspondência de padrões, além de permitir proteção automatizada contra riscos associados.

AWS KMS

AWS KMScria e controla as chaves criptográficas que você usa para proteger seus dados.

AWS CloudHSM

AWS CloudHSMfornece módulos de segurança de hardware altamente disponíveis e baseados em nuvem ()HSMs.

AWS Certificate Manager

AWS Certificate Managerlida com a complexidade de criar, armazenar e renovar certificados e chaves SSL/TLS X.509 públicos e privados.

AWS Private CA

AWS Private CAajuda você a criar hierarquias de autoridade de certificação privadas, incluindo autoridades de certificação raiz e subordinadas (). CAs

AWS Secrets Manager

AWS Secrets Managerajuda você a gerenciar, recuperar e alternar credenciais de banco de dados, credenciais de aplicativos, OAuth tokens, chaves de API e outros segredos.

AWS Payment Cryptography

AWS Payment Cryptographyfornece acesso às funções criptográficas e ao gerenciamento de chaves usados no processamento de pagamentos de acordo com os padrões do setor de cartões de pagamento (PCI).

AWS Entenda os serviços de proteção de rede e aplicativos

AWS oferece vários serviços para proteger suas redes e aplicativos. AWS Shieldfornece proteção contra ataques distribuídos de negação de serviço (DDoS) e AWS WAFajuda a proteger aplicativos da Web contra ataques comuns de exploração da Web.

A tabela a seguir resume as ofertas de proteção de rede e aplicativos discutidas neste guia:

AWS Firewall Manager

AWS Firewall Managersimplifica suas tarefas de administração e manutenção em várias contas e recursos para proteção.

AWS Network Firewall

AWS Network Firewallfornece um firewall de rede gerenciado e com monitoramento de estado e um serviço de detecção e prevenção de intrusões com sua VPC.

AWS Shield

AWS Shieldfornece proteções contra ataques DDo S para AWS recursos nas camadas de rede, transporte e aplicação.

AWS WAF

AWS WAFfornece um firewall de aplicativo web para que você possa monitorar as solicitações HTTP (S) que são encaminhadas para seus recursos protegidos de aplicativos web.

Entenda os serviços de AWS detecção e resposta

AWS fornece ferramentas para ajudá-lo a simplificar as operações de segurança em todo o seu AWS ambiente, incluindo ambientes com várias contas. Por exemplo, você pode usar a Amazon GuardDuty para detecção inteligente de ameaças e usar o Amazon Detective para identificar e analisar descobertas de segurança coletando dados de log. AWS Security Huboferece suporte a vários padrões de segurança e fornece uma visão geral dos alertas de segurança e do status de conformidade em todo o mundo Contas da AWS. AWS CloudTrailrastreia a atividade do usuário e o uso da interface de programação de aplicativos (API), o que é crucial para entender e responder aos eventos de segurança.

A tabela a seguir resume as ofertas de detecção e resposta discutidas neste guia:

AWS Config

AWS Configfornece uma visão detalhada da configuração dos AWS recursos em seu Conta da AWS.

AWS CloudTrail

AWS CloudTrailregistra ações realizadas por um usuário, função ou AWS service (Serviço da AWS).

AWS Security Hub

AWS Security Hubfornece uma visão abrangente do seu estado de segurança em AWS.

Amazon GuardDuty

A Amazon monitora GuardDuty continuamente suas cargas de trabalho Contas da AWS, atividades de tempo de execução e dados em busca de atividades maliciosas.

Amazon Inspector

O Amazon Inspector escaneia suas AWS cargas de trabalho em busca de vulnerabilidades de software e exposição não intencional na rede.

Amazon Security Lake

O Amazon Security Lake centraliza automaticamente dados de segurança de AWS ambientes, provedores de SaaS, ambientes locais, fontes de nuvem e fontes de terceiros em um data lake.

Amazon Detective

O Amazon Detective ajuda a analisar, investigar e identificar rapidamente a causa raiz de descobertas de segurança ou atividades suspeitas.

AWS Security Incident Response

AWS Resposta a incidentes de segurança

Ajuda você a se preparar, responder e receber orientações rapidamente para ajudar na recuperação de incidentes de segurança.

AWS Entenda os serviços de governança e conformidade

AWS fornece ferramentas que ajudam você a aderir aos seus padrões de segurança, operacionais, de conformidade e de custo. Por exemplo, você pode usar AWS Control Towerpara configurar e controlar um ambiente de várias contas com controles prescritivos. Com AWS Organizations, você pode configurar o gerenciamento baseado em políticas para várias contas em sua organização.

AWS também oferece uma visão abrangente do status de conformidade e monitora continuamente seu ambiente usando verificações de conformidade automatizadas com base nas AWS melhores práticas e nos padrões do setor que sua organização segue. Por exemplo, AWS Artifactfornece acesso sob demanda a relatórios de conformidade e AWS Audit Managerautomatiza a coleta de

evidências para que você possa avaliar com mais facilidade se seus controles estão operando de forma eficaz.

A tabela a seguir resume as ofertas de governança e conformidade discutidas neste guia:

AWS Organizations

AWS Organizationsajuda você a consolidar vários Contas da AWS em uma organização que você cria e gerencia centralmente.

AWS Control Tower

AWS Control Towerajuda você a configurar e administrar um ambiente de AWS várias contas baseado nas melhores práticas.

AWS Artifact

AWS Artifactfornece downloads sob demanda de documentos de AWS segurança e conformidade.

AWS Audit Manager

AWS Audit Manager

Ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você avalia o risco e a conformidade.

Considere os critérios de AWS segurança, identidade e governança

A escolha dos serviços certos de segurança, identidade e governança AWS depende de seus requisitos e casos de uso específicos. A decisão de adotar um serviço AWS de segurança fornece uma árvore de decisão para ajudá-lo a decidir se a adoção Serviços da AWS por motivos de segurança, identidade e governança é adequada para sua organização. Além disso, aqui estão alguns critérios a serem considerados ao tomar sua decisão sobre quais serviços usar.

Security requirements and threat landscape

Faça uma avaliação abrangente das vulnerabilidades e ameaças específicas da sua organização. Isso envolve identificar os tipos de dados que você manipula, como informações pessoais de clientes, registros financeiros ou dados comerciais proprietários. Entenda os riscos potenciais associados a cada um.

Avalie sua arquitetura de aplicativos e infraestrutura. Determine se seus aplicativos são voltados para o público e que tipo de tráfego da web eles manipulam. Isso influencia sua necessidade de serviços como proteção contra AWS WAF a exploração da web. Para aplicativos internos, considere a importância da detecção interna de ameaças e do monitoramento contínuo com a Amazon GuardDuty, que pode identificar padrões de acesso incomuns ou implantações não autorizadas.

Por fim, considere a sofisticação de sua postura de segurança existente e a experiência de sua equipe de segurança. Se sua equipe tem recursos limitados, escolher serviços que ofereçam mais automação e integração pode fornecer aprimoramentos de segurança eficazes, sem sobrecarregar sua equipe. Exemplos de serviços incluem AWS Shield proteção DDo S e AWS Security Hub monitoramento centralizado de segurança.

Compliance and regulatory requirements

Identifique as leis e padrões relevantes para seu setor ou região geográfica, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos EUA de 1996 (HIPAA) ou o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS).

AWS oferece serviços como o AWS Config AWS Artifact para ajudá-lo a gerenciar a conformidade com vários padrões. Com AWS Config, você pode avaliar, auditar e avaliar as configurações de seus AWS recursos, facilitando a garantia da conformidade com as políticas internas e os requisitos normativos. AWS O Artifact fornece acesso sob demanda à documentação de AWS conformidade, ajudando você com auditorias e relatórios de conformidade.

A escolha de serviços que se alinhem às suas necessidades específicas de conformidade pode ajudar sua organização a atender aos requisitos legais e criar um ambiente seguro e confiável para seus dados. Explore os programas de AWS conformidade para saber mais.

Scalability and flexibility

Considere como sua organização crescerá e com que rapidez. Escolha Serviços da AWS isso que ajudará suas medidas de segurança a crescerem perfeitamente com sua infraestrutura e a se adaptarem às ameaças em evolução.

Para ajudar você a escalar rapidamente, AWS Control Tower orquestra os recursos de vários outros Serviços da AWS, incluindo AWS Organizations o AWS IAM Identity Center, para criar uma landing zone em menos de uma hora. A Control Tower configura e gerencia recursos em seu nome.

AWS também projeta muitos serviços para escalar automaticamente de acordo com os padrões de tráfego e uso de um aplicativo, como o Amazon, GuardDuty para detecção de ameaças e AWS WAF proteção de aplicativos da web. À medida que sua empresa cresce, esses serviços se expandem com ela, sem exigir ajustes manuais ou causar gargalos.

Além disso, é fundamental que você possa personalizar seus controles de segurança para atender aos requisitos de sua empresa e aos cenários de ameaças. Considere gerenciar suas contas com AWS Organizations, para que você possa gerenciar mais de 40 recursos de serviços em várias contas. 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 oferecer governança e visibilidade às equipes de segurança centralizadas.

Considerar a escalabilidade e a flexibilidade ajuda a garantir que sua postura de segurança seja robusta, responsiva e capaz de suportar ambientes de negócios dinâmicos.

Integration with existing systems

Considere medidas de segurança que aprimorem, em vez de interromper, suas operações atuais. Por exemplo, considere o seguinte:

- Simplifique seus fluxos de trabalho agregando dados e alertas de segurança Serviços da AWS e analisando-os junto com os sistemas de gerenciamento de eventos e informações de segurança (SIEM) existentes.
- Crie uma visão unificada das ameaças e vulnerabilidades de segurança em ambientes locais AWS e em ambos os ambientes.
- Integre-se AWS CloudTrail às soluções de gerenciamento de registros existentes para um monitoramento abrangente das atividades do usuário e do uso da API em toda a sua AWS infraestrutura e aplicativos existentes.
- Examine maneiras de otimizar a utilização de recursos e aplicar políticas de segurança de forma consistente em todos os ambientes. Isso ajuda a reduzir o risco de falhas na cobertura de segurança.

Cost and budget considerations

Analise os modelos de preços para cada serviço que você está considerando. AWS geralmente cobram com base no uso, como o número de chamadas de API, o volume de dados processados ou a quantidade de dados armazenados. Por exemplo, a Amazon GuardDuty cobra com base na quantidade de dados de log analisados para detecção de ameaças, enquanto AWS WAF as

faturas são baseadas no número de regras implantadas e no número de solicitações da web recebidas.

Faça uma estimativa do uso esperado para prever os custos com precisão. Considere as necessidades atuais e o crescimento potencial ou os picos na demanda. Por exemplo, a escalabilidade é um recurso fundamental Serviços da AWS, mas também pode levar ao aumento de custos se não for gerenciada com cuidado. Use o AWS Calculadora de Preçospara modelar diferentes cenários e avaliar seu impacto financeiro.

Avalie o custo total de propriedade (TCO), que inclui custos diretos e indiretos, como o tempo e os recursos necessários para gerenciamento e manutenção. Optar por serviços gerenciados pode reduzir a sobrecarga operacional, mas pode ter um preço mais alto.

Por fim, priorize seus investimentos em segurança com base na avaliação de riscos. Nem todos os serviços de segurança serão igualmente essenciais para sua infraestrutura, portanto, concentre seu orçamento nas áreas que terão o impacto mais significativo na redução de riscos e na garantia da conformidade. Equilibrar a relação custo-benefício com o nível de segurança de que você precisa é fundamental para uma estratégia de AWS segurança bem-sucedida.

Organizational structure and access needs

Avalie como sua organização está estruturada e opera, e como suas necessidades de acesso podem variar de acordo com a equipe, o projeto ou o local. Isso influencia na forma como você gerencia e autentica identidades de usuários, atribui funções e aplica controles de acesso em todo o seu ambiente. AWS Implemente as melhores práticas, como aplicar permissões com privilégios mínimos e exigir autenticação multifator (MFA).

A maioria das organizações precisa de um ambiente com várias contas. Analise as melhores práticas para esse tipo de ambiente e considere usá-lo AWS Organizations e ajudá-lo AWS Control Tower a implementá-lo.

Outro aspecto que você deve considerar é o gerenciamento de credenciais e chaves de acesso. Considere usar o IAM Identity Center para centralizar o gerenciamento de acesso em vários aplicativos Contas da AWS e aplicativos comerciais, o que aumenta a segurança e a conveniência do usuário. Para ajudar você a gerenciar facilmente o acesso às contas da sua organização, o IAM Identity Center se integra com o. AWS Organizations

Além disso, avalie como esses serviços de gerenciamento de identidade e acesso se integram aos seus serviços de diretório existentes. Se você tiver um provedor de identidade existente, poderá integrá-lo ao IAM Identity Center usando SAML 2.0 ou OpenID Connect (OIDC). O IAM

Identity Center também tem suporte para o provisionamento do System for Cross-domain Identity Management (SCIM) para ajudar a manter seus diretórios sincronizados. Isso ajuda você a garantir uma experiência de usuário perfeita e segura ao acessar AWS os recursos.

Escolha um serviço AWS de segurança, identidade e governança

Agora que você conhece os critérios para avaliar suas opções de segurança, está pronto para escolher quais serviços AWS de segurança podem ser adequados às suas necessidades organizacionais.

A tabela a seguir destaca quais serviços são otimizados para quais circunstâncias. Use a tabela para ajudar a determinar o serviço mais adequado para sua organização e caso de uso.

> **Note**
>
> [1] Integra-se com AWS Security Hub (lista completa)
> [2] Integra-se com a Amazon GuardDuty (lista completa)
> [3] Integra-se ao Amazon Security Lake (lista completa)

Escolha serviços de gerenciamento de AWS identidade e acesso

Conceda às pessoas apropriadas o nível adequado de acesso a sistemas, aplicativos e dados.

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de segurança, identidade e governança
Use esses serviços para ajudá-lo a gerenciar e controlar com segurança o acesso de seus clientes, força de trabalho e cargas de trabalho.	Ajuda você a conectar sua fonte de identidades ou criar usuários. Você pode gerenciar centralmente o acesso da força de trabalho a várias AWS contas e aplicativos.	AWS IAM Identity Center
	Otimizado para autentica r e autorizar usuários para aplicativos web e móveis.	Amazon Cognito

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de segurança, identidade e governança
	Otimizado para compartil har recursos internos com segurança. AWS	AWS RAM
	Permite um controle seguro e refinado sobre o acesso aos AWS recursos da carga de trabalho.	IAM [1]

Escolha serviços AWS de proteção de dados

Automatize e simplifique as tarefas de proteção e segurança de dados que vão desde o gerenciamento de chaves e a descoberta de dados confidenciais até o gerenciamento de credenciais.

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de proteção de dados
Use esses serviços para ajudá-lo a alcançar e manter a confidencialidade, integrida de e disponibilidade de dados confidenciais armazenad os e processados em AWS ambientes.	Otimizado para descobrir dados confidenciais.	Amazon Macie [1]
	Otimizado para chaves criptográficas.	AWS KMS
	Otimizado para HSMs.	AWS CloudHSM
	Otimizado para certificados e SSL/TLS chaves X.509 privados.	AWS Certificate Manager
	Otimizado para criar hierarqui as de autoridade de certifica ção privadas.	AWS Private CA

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de proteção de dados
	Otimizado para credenciais de banco de dados, credenciais de aplicativos, OAuth tokens, chaves de API e outros segredos.	AWS Secrets Manager
	Otimizado para fornecer acesso às funções criptográficas e ao gerenciamento de chaves usadas no processamento de pagamentos de acordo com os padrões PCI.	AWS Payment Cryptography

Escolha serviços de proteção de AWS rede e aplicativos

Proteja centralmente seus recursos da Internet contra ataques comuns DDo de S e aplicativos.

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de proteção de rede e aplicativos
Use esses serviços para ajudá-lo a aplicar políticas de segurança detalhadas em cada ponto de controle da rede.	Otimizado para configurar e gerenciar centralmente as regras de firewall.	AWS Firewall Manager[1]
	Otimizado para fornecer um firewall de rede gerenciado e com monitoramento de estado e serviço de detecção e prevenção de intrusões.	AWS Network Firewall
	Otimizado para proteção contra ataques DDo S para AWS recursos nas	AWS Shield

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de proteção de rede e aplicativos
	camadas de rede, transporte e aplicação.	
	Otimizado para fornecer um firewall de aplicativos da web.	AWS WAF

Escolha serviços AWS de detecção e resposta

Identifique e priorize continuamente os riscos de segurança e, ao mesmo tempo, integre as melhores práticas de segurança com antecedência.

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de detecção e resposta
Use esses serviços para ajudá-lo a detectar e responder aos riscos de segurança em suas contas, para que você possa proteger suas cargas de trabalho em grande escala.	Otimizado para automatizar verificações de segurança e centralizar alertas de segurança com AWS integrações de terceiros.	AWS Security Hub[2, 3]
	Otimizado para avaliar, auditar e avaliar a configuração de seus recursos.	AWS Config[1]
	Otimizado para registrar eventos de outros Serviços da AWS como uma trilha de auditoria.	AWS CloudTrail
	Otimizado para detecção inteligente de ameaças e relatórios detalhados.	Amazon GuardDuty [1]
	Otimizado para gerenciamento de vulnerabilidades.	Amazon Inspector 1

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de detecção e resposta
	Otimizado para centralizar dados de segurança.	Lago de Segurança da Amazon [1]
	Otimizado para agregar e resumir possíveis problemas de segurança.	Detective Amazon [1, 2, 3]
	Otimizado para ajudar você a fazer a triagem de descobertas, escalar eventos de segurança e gerenciar casos que exigem sua atenção imediata.	AWS Resposta a incidentes de segurança

Escolha serviços de AWS governança e conformidade

Estabeleça a governança da nuvem em todos os seus recursos e automatize seus processos de conformidade e auditoria.

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de governança e conformidade
Use esses serviços para ajudá-lo a implementar as melhores práticas e atender aos padrões do setor ao usar AWS.	Otimizado para gerenciar centralmente várias contas e faturamento consolidado.	AWS Organizations
	Otimizado para fornecer downloads sob demanda de documentos de AWS segurança e conformidade.	AWS Artifact
	Otimizado para AWS uso de auditoria.	AWS Audit Manager[1]

Quando você deve usá-lo?	Para que ele é otimizado?	Serviços de governança e conformidade
	Otimizado para configurar e governar um ambiente AWS com várias contas.	AWS Control Tower

Use serviços AWS de segurança, identidade e governança

Agora você deve ter uma compreensão clara do que cada serviço de AWS segurança, identidade e governança (e das AWS ferramentas e serviços de suporte) faz e quais podem ser adequados para você.

Para explorar como usar e aprender mais sobre cada um dos serviços de AWS segurança, identidade e governança disponíveis, fornecemos um caminho para explorar como cada um dos serviços funciona. As seções a seguir fornecem links para documentação detalhada, tutoriais práticos e recursos para você começar.

Use serviços de gerenciamento de AWS identidade e acesso

As tabelas a seguir mostram alguns recursos úteis de gerenciamento de identidade e acesso, organizados por serviço, para ajudar você a começar.

AWS IAM Identity Center

- Habilitando o AWS IAM Identity Center

  Ative o IAM Identity Center e comece a usá-lo com seu AWS Organizations.

  Explore o guia
- Configure o acesso do usuário com o diretório padrão do IAM Identity Center

  Use o diretório padrão como sua fonte de identidade e configure e teste o acesso do usuário.

  Comece a usar o tutorial
- Usando o Active Directory como fonte de identidade

Conclua a configuração básica para usar o Active Directory como fonte de identidade do IAM Identity Center.

Comece a usar o tutorial

- Configurar SAML e SCIM com Okta e IAM Identity Center

  Configure uma conexão SAML com o Okta e o IAM Identity Center.

  Comece a usar o tutorial

Amazon Cognito

- Comece a usar o Amazon Cognito

  Saiba mais sobre as tarefas mais comuns do Amazon Cognito.

  Explore o guia
- Tutorial: Criando um grupo de usuários

  Crie um grupo de usuários, que permita que seus usuários façam login no seu aplicativo web ou móvel.

  Comece a usar o tutorial
- Tutorial: Criando um pool de identidades

  Crie um pool de identidades, que permita que seus usuários obtenham AWS credenciais temporárias para acessar Serviços da AWS.

  Comece a usar o tutorial
- Workshop sobre o Amazon Cognito

  Pratique o uso do Amazon Cognito para criar uma solução de autenticação para uma loja de animais hipotética.

  Comece a usar o tutorial

AWS RAM

- Começando com AWS RAM

Saiba mais sobre AWS RAM termos e conceitos.

Explore o guia

- Trabalhando com AWS recursos compartilhados

  Compartilhe AWS recursos que você possui e acesse AWS recursos que são compartilhados com você.

  Explore o guia

- Gerenciando permissões na AWS RAM

  Saiba mais sobre os dois tipos de permissões gerenciadas: permissões AWS gerenciadas e permissões gerenciadas pelo cliente.

  Explore o guia

- Configure o acesso detalhado aos seus recursos que são compartilhados usando AWS RAM

  Use as permissões gerenciadas pelo cliente para personalizar seu acesso aos recursos e obter a melhor prática de privilégios mínimos.

  Leia o blog

IAM

- Começando a usar o IAM

  Crie funções, usuários e políticas do IAM usando AWS Management Console o.

  Comece a usar o tutorial

- Delegar acesso ao Contas da AWS uso de funções

  Use uma função para delegar acesso a recursos diferentes Contas da AWS da sua, chamada Produção e Desenvolvimento.

  Comece a usar o tutorial

- Crie uma política gerenciada pelo cliente

  Use o AWS Management Console para criar uma política gerenciada pelo cliente e, em seguida, anexe essa política a um usuário do IAM em seu Conta da AWS.

Comece a usar o tutorial

- Defina permissões para acessar AWS recursos com base em tags

  Crie e teste uma política que permita que funções do IAM com tags principais acessem recursos com tags correspondentes.

  Comece a usar o tutorial

- Práticas recomendadas de segurança no IAM

  Ajude a proteger seus AWS recursos usando as melhores práticas do IAM.

  Explore o guia

Use serviços AWS de proteção de dados

A seção a seguir fornece links para recursos detalhados que descrevem a proteção AWS de dados.

Macie

- Conceitos básicos do Amazon Macie

  Habilite o Macie para você Conta da AWS, avalie sua postura de segurança do Amazon S3 e defina as principais configurações e recursos para descobrir e relatar dados confidenciais em seus buckets do S3.

  Explore o guia

- Monitorando a segurança e a privacidade dos dados com o Amazon Macie

  Use o Amazon Macie para monitorar a segurança de dados do Amazon S3 e avaliar sua postura de segurança.

  Explore o guia

- Analisando as descobertas do Amazon Macie

  Analise, analise e gerencie as descobertas do Amazon Macie.

  Explore o guia

- Recuperação de amostras de dados confidenciais com as descobertas do Amazon Macie

Use o Amazon Macie para recuperar e revelar amostras de dados confidenciais que são relatados por descobertas individuais.

Explore o guia

- Descobrindo dados confidenciais com o Amazon Macie

  Automatize a descoberta, o registro e a emissão de relatórios de dados confidenciais em seu patrimônio de dados do Amazon S3.

  Explore o guia

AWS KMS

- Começando com AWS KMS

  Gerencie chaves KMS de criptografia simétrica, da criação à exclusão.

  Explore o guia

- Chaves para fins especiais

  Saiba mais sobre os diferentes tipos de chaves que oferecem AWS KMS suporte, além das chaves KMS de criptografia simétrica.

  Explore o guia

- Dimensionando seus recursos de criptografia em repouso com AWS KMS

  Saiba mais sobre as opções de criptografia em repouso disponíveis em AWS.

  Explore o workshop

AWS CloudHSM

- Começando com AWS CloudHSM

  Crie, inicialize e ative um AWS CloudHSM cluster.

  Explore o guia

- Gerenciando AWS CloudHSM clusters

Conecte-se ao seu AWS CloudHSM cluster e às várias tarefas administrativas no gerenciamento do seu cluster.

Explore o guia

- Gerenciando usuários e chaves do HSM no AWS CloudHSM

  Crie usuários e chaves HSMs no seu cluster.

  Explore o guia

- Automatize a implantação de um serviço web NGINX usando o Amazon ECS com descarregamento de TLS no CloudHSM

  Use AWS CloudHSM para armazenar suas chaves privadas para seus sites hospedados na nuvem.

  Leia o blog

AWS Certificate Manager

- Solicitando um certificado público

  Use o console AWS Certificate Manager (ACM) ou AWS CLI solicite um certificado público do ACM.

  Explore o guia

- Práticas recomendadas para AWS Certificate Manager

  Conheça as melhores práticas com base na experiência real dos clientes atuais da ACM.

  Explore o guia

- Como usar AWS Certificate Manager para impor controles de emissão de certificados

  Use as chaves de condição do IAM para garantir que seus usuários estejam emitindo ou solicitando certificados TLS de acordo com as diretrizes da sua organização.

  Leia o blog

AWS Private CA

- Planejando sua AWS Private CA implantação

  Prepare-se AWS Private CA para uso antes de criar uma autoridade de certificação privada.

  Explore o guia
- AWS Private CA administração

  Crie uma hierarquia totalmente AWS hospedada de autoridades de certificação raiz e subordinadas para uso interno de sua organização.

  Explore o guia
- Administração de certificados

  Execute tarefas básicas de administração de certificados com AWS Private CA, como emitir, recuperar e listar certificados privados.

  Explore o guia
- AWS Private CA oficina

  Desenvolva experiência prática com vários casos de uso de autoridades de certificação privadas.

  Explore o workshop
- Como simplificar o provisionamento de certificados no Active Directory com AWS Private CA

  Use AWS Private CA para provisionar certificados com mais facilidade para usuários e máquinas em seu ambiente Microsoft Active Directory.

  Leia o blog
- Como impor restrições de nome DNS em AWS Private CA

  Aplique restrições de nome DNS a uma CA subordinada usando o serviço. AWS Private CA

  Leia o blog

AWS Secrets Manager

- AWS Secrets Manager conceitos

Execute tarefas básicas de administração de certificados com AWS Private CA, como emitir, recuperar e listar certificados privados.

Explore o guia

- Configure a rotação alternada de usuários para AWS Secrets Manager

  Configure uma rotação alternada de usuários para um segredo que contenha credenciais de banco de dados.

  Explore o guia

- Usando AWS Secrets Manager segredos com o Kubernetes

  Mostre segredos do Secrets Manager como arquivos montados em pods do Amazon EKS usando o AWS Secrets and Configuration Provider (ASCP).

  Explore o guia

AWS Payment Cryptography

- Começando com AWS Payment Cryptography

  Crie chaves e use-as em várias operações criptográficas.

  Explore o guia

- AWS Payment Cryptography FAQs

  Entenda o básico do. AWS Payment Cryptography

  Explore o FAQs

Use serviços de proteção de AWS rede e aplicativos

As tabelas a seguir fornecem links para recursos detalhados que descrevem a proteção de AWS redes e aplicativos.

AWS Firewall Manager

- Introdução às AWS Firewall Manager políticas

Use AWS Firewall Manager para ativar diferentes tipos de políticas de segurança.

Explore o guia

- Como auditar e limitar continuamente os grupos de segurança com AWS Firewall Manager

  Use AWS Firewall Manager para limitar os grupos de segurança, garantindo que somente as portas necessárias estejam abertas.

  Leia o blog

- Use AWS Firewall Manager para implantar proteção em grande escala em AWS Organizations

  Use AWS Firewall Manager para implantar e gerenciar políticas de segurança em todo o seu AWS Organizations.

  Leia o blog

AWS Network Firewall

- Começando com AWS Network Firewall

  Configure e implemente um AWS Network Firewall firewall para uma VPC com uma arquitetura básica de gateway de internet.

  Explore o guia

- AWS Network Firewall Workshop

  Implemente e AWS Network Firewall usando a infraestrutura como código.

  Explore o workshop

- Passo a passo prático do mecanismo de regras AWS Network Firewall flexíveis — Parte 1

  Implante uma demonstração de AWS Network Firewall dentro de você Conta da AWS para interagir com seu mecanismo de regras.

  Leia o blog

- Passo a passo prático do mecanismo de regras AWS Network Firewall flexíveis — Parte 2

  Crie uma política de firewall com uma ordem de regras estrita e defina uma ou mais ações padrão.

Leia o blog

- Modelos de implantação para AWS Network Firewall

  Aprenda modelos de implantação para casos de uso comuns nos quais você pode adicionar AWS Network Firewall ao caminho do tráfego.

  Leia o blog

- Modelos de implantação AWS Network Firewall com aprimoramentos de roteamento de VPC

  Use primitivas de roteamento de VPC aprimoradas para inserir AWS Network Firewall entre cargas de trabalho em diferentes sub-redes da mesma VPC.

  Leia o blog

AWS Shield

- Como AWS Shield funciona

  Saiba como AWS Shield Standard e AWS Shield Advanced forneça proteções contra ataques DDo S para AWS recursos nas camadas de rede e transporte (camadas 3 e 4) e na camada de aplicação (camada 7).

  Explore o guia

- Começando com AWS Shield Advanced

  Comece AWS Shield Advanced usando o console Shield Advanced.

  Explore o guia

- AWS Shield Advanced oficina

  Proteja os recursos expostos à Internet contra ataques DDo S, monitore DDo os ataques S contra sua infraestrutura e notifique as equipes apropriadas.

  Explore o workshop

AWS WAF

- Começando com AWS WAF

Configure AWS WAF, crie uma ACL da web e proteja a Amazon CloudFront adicionando regras e grupos de regras para filtrar solicitações da web.

Comece a usar o tutorial

- Análise de AWS WAF registros no Amazon CloudWatch Logs

  Configure o AWS WAF registro nativo CloudWatch nos registros da Amazon e visualize e analise os dados nos registros.

  Leia o blog
- Visualize AWS WAF registros com um painel da Amazon CloudWatch

  Use CloudWatch a Amazon para monitorar e analisar AWS WAF atividades usando CloudWatch métricas, Contributor Insights e Logs Insights.

  Leia o blog

Use serviços AWS de detecção e resposta

As tabelas a seguir fornecem links para recursos detalhados que descrevem os serviços AWS de detecção e resposta.

AWS Config

- Começando com AWS Config

  Configure AWS Config e trabalhe com AWS SDKs.

  Explore o guia
- Workshop de risco e conformidade

  Automatize os controles usando regras AWS Config de configuração AWS gerenciadas.

  Explore o workshop
- AWS Config Biblioteca de kits de desenvolvimento de regras: crie e opere regras em grande escala

  Use o Rule Development Kit (RDK) para criar uma AWS Config regra personalizada e implantá-la com o. RDKLib

Leia o blog

AWS CloudTrail

- Exibir histórico de eventos

  Analise a atividade da AWS API em seus Conta da AWS serviços compatíveis CloudTrail.

  Comece a usar o tutorial
- Crie uma trilha para registrar eventos de gerenciamento

  Crie uma trilha para registrar eventos de gerenciamento em todas as regiões.

  Comece a usar o tutorial

AWS Security Hub

- Habilitando AWS Security Hub

  Ative AWS Security Hub com AWS Organizations ou em uma conta independente.

  Explore o guia
- Agregação entre regiões

  Agregue AWS Security Hub descobertas de várias Regiões da AWS para uma única região de agregação.

  Explore o guia
- AWS Security Hub oficina

  Aprenda a usar, gerenciar AWS Security Hub e melhorar a postura de segurança de seus AWS ambientes.

  Explore o workshop
- Três padrões de uso recorrentes do Security Hub e como implantá-los

  Saiba mais sobre os três padrões de AWS Security Hub uso mais comuns e como melhorar sua estratégia para identificar e gerenciar descobertas.

Leia o blog

Amazon GuardDuty

- Começando com a Amazon GuardDuty

  Habilite a Amazon GuardDuty, gere amostras de resultados e configure alertas.

  Explore o tutorial

- Proteção EKS na Amazon GuardDuty

  Use GuardDuty a Amazon para monitorar seus registros de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS).

  Explore o guia

- Proteção Lambda na Amazon GuardDuty

  Identifique possíveis ameaças à segurança ao invocar uma AWS Lambda função.

  Explore o guia

- GuardDuty Proteção do Amazon RDS

  Use GuardDuty a Amazon para analisar e traçar o perfil da atividade de login do Amazon Relational Database Service (Amazon RDS) para possíveis ameaças de acesso aos seus bancos de dados Amazon Aurora.

  Explore o guia

- Proteção do Amazon S3 na Amazon GuardDuty

  Use GuardDuty para monitorar eventos CloudTrail de dados e identificar possíveis riscos de segurança em seus buckets do S3.

  Explore o guia

- Detecção e resposta a ameaças com a Amazon GuardDuty e o Amazon Detective

  Aprenda os conceitos básicos da Amazon GuardDuty e do Amazon Detective.

  Explore o workshop

Amazon Inspector

- Introdução ao Amazon Inspector

  Ative as verificações do Amazon Inspector para entender as descobertas no console.

  Comece a usar o tutorial

- Gestão de vulnerabilidades com o Amazon Inspector

  Use o Amazon Inspector para escanear EC2 instâncias da Amazon e imagens de contêineres no Amazon Elastic Container Registry (Amazon ECR) em busca de vulnerabilidades de software.

  Explore o workshop

- Como escanear EC2 AMIs usando o Amazon Inspector

  Crie uma solução usando várias Serviços da AWS para verificar suas AMIs vulnerabilidades conhecidas.

  Leia o blog

Amazon Security Lake

- Introdução ao Amazon Security Lake

  Ative e comece a usar o Amazon Security Lake.

  Explore o guia

- Gerenciando várias contas com AWS Organizations

  Colete registros e eventos de segurança de vários Contas da AWS.

  Explore o guia

- Ingira, transforme e entregue eventos publicados pelo Amazon Security Lake para o Amazon Service OpenSearch

  Ingira, transforme e entregue dados do Amazon Security Lake ao Amazon OpenSearch Service para uso por suas SecOps equipes.

  Leia o blog

- Como visualizar as descobertas do Amazon Security Lake com QuickSight

  Consulte e visualize dados do Amazon Security Lake usando o Amazon QuickSight Athena e.

  Leia o blog

Amazon Detective

- Termos e conceitos do Amazon Detective

  Aprenda os principais termos e conceitos que são importantes para entender o Amazon Detective e como ele funciona.

  Explore o guia
- Configurando o Amazon Detective

  Habilite o Amazon Detective a partir do console Amazon Detective, da API Amazon Detective ou. AWS CLI

  Explore o guia
- Detecção e resposta a ameaças com a Amazon GuardDuty e o Amazon Detective

  Aprenda os conceitos básicos da Amazon GuardDuty e do Amazon Detective.

  Explore o workshop

Use serviços de AWS governança e conformidade

As tabelas a seguir fornecem links para recursos detalhados que descrevem a governança e a conformidade.

AWS Organizations

- Criando e configurando uma organização

  Crie sua organização e configure-a com duas contas de AWS membros.

  Comece a usar o tutorial
- Serviços que funcionam com AWS Organizations

Entenda com o que Serviços da AWS você pode usar AWS Organizations e os benefícios de usar cada serviço em toda a organização.

Explore o guia

- Organizando seu AWS ambiente usando várias contas

  Implemente as melhores práticas e as recomendações atuais para organizar seu AWS ambiente geral.

  Leia o whitepaper

AWS Artifact

- Começando com AWS Artifact

  Baixe relatórios de segurança e conformidade, gerencie contratos legais e gerencie notificações.

  Explore o guia

- Gerenciando contratos em AWS Artifact

  Use o AWS Management Console para revisar, aceitar e gerenciar contratos para sua conta ou organização.

  Explore o guia

- Prepare-se para uma auditoria na AWS Parte 1 — AWS Audit Manager e AWS Artifact AWS Config

  Use Serviços da AWS para ajudá-lo a automatizar a coleta de evidências usadas em auditorias.

  Leia o blog

AWS Audit Manager

- Habilitando o AWS Audit Manager

  Ative o Audit Manager usando o AWS Management Console, a API do Audit Manager ou AWS CLI o.

Explore o guia

- Tutorial para proprietários de auditoria: Criando uma avaliação

  Crie uma avaliação usando o Audit Manager Sample Framework.

  Explore o guia

- Tutorial para delegados: revisando um conjunto de controles

  Revise um conjunto de controle que foi compartilhado com você por um proprietário de auditoria no Audit Manager.

  Explore o guia

AWS Control Tower

- Começando com AWS Control Tower

  Configure e lance um ambiente com várias contas, chamado landing zone, que siga as melhores práticas prescritivas.

  Explore o guia

- Modernizando o gerenciamento de contas com o Amazon Bedrock e AWS Control Tower

  Provisione uma conta de ferramentas de segurança e aproveite a IA generativa para agilizar o processo de Conta da AWS configuração e gerenciamento.

  Leia o blog

- Construindo um ambiente bem arquitetado AWS GovCloud (EUA) com AWS Control Tower

  Configure sua governança nas regiões AWS GovCloud (EUA), incluindo o controle de suas AWS cargas de trabalho usando unidades organizacionais (OUs) e. Contas da AWS

  Leia o blog

Explore os serviços de AWS segurança, identidade e governança

Editable architecture diagrams

Diagramas de arquitetura de referência

Explore diagramas de arquitetura de referência para ajudá-lo a desenvolver sua estratégia de segurança, identidade e governança.

Explore arquiteturas de referência de segurança, identidade e governança

Ready-to-use code

Solução em destaque

Insights de segurança sobre AWS

Implante um código AWS criado para ajudar você a visualizar dados no Amazon Security Lake para investigar e responder mais rapidamente aos eventos de segurança.

Explore esta solução

AWS Soluções

Explore soluções pré-configuradas e implantáveis e seus guias de implementação, criados por. AWS

Explore todas as soluções AWS de segurança, identidade e governança

Documentation

Whitepapers sobre segurança, identidade e governança

Explore os whitepapers para obter mais informações e melhores práticas sobre como escolher, implementar e usar os serviços de segurança, identidade e governança que melhor se adequam à sua organização.

Explore os whitepapers sobre segurança, identidade e governança

AWS Blog de segurança

Explore postagens de blog que abordam casos de uso de segurança específicos.

Explore o blog AWS de segurança

Histórico do documento

A tabela a seguir descreve as mudanças importantes nesse guia de decisão. Para receber notificações sobre atualizações deste guia, você pode assinar um feed RSS.

Alteração	Descrição	Data
Atualização do re:Invent	Foram adicionadas informaçõ es sobre Resposta a Incidente s de AWS Segurança AWS Payment Cryptography e. Informações de serviço atualizadas para AWS Identity and Access Management AWS IAM Identity Center e.	30 de dezembro de 2024
Atualização de vídeo	Vídeo introdutório atualizado com uma palestra relâmpago recente do re:inforce 2024.	25 de junho de 2024
Serviços de governança adicionados	Ampliou o escopo do documento para incluir governança, incluindo adição de AWS CloudTrail AWS Control Tower, e. AWS Organizations Gráficos atualizados para refletir o novo escopo. Melhores práticas de identidade esclarecidas. Alterações editoriais de modo geral.	7 de junho de 2024
Publicação inicial	Guia publicado pela primeira vez.	21 de março de 2024

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.