AWS Guia de decisão

Escolhendo um AWS serviço de criptografia

Escolhendo um AWS serviço de criptografia: AWS Guia de decisão

Table of Contents

Escolhendo um AWS serviço de criptografia

Dando o primeiro passo

Finalidade	Ajude a determinar quais serviços de AWS criptografia são mais adequados para sua organização.
Última atualização	31 de janeiro de 2025
Serviços cobertos	• AWS Certificate Manager • AWS CloudHSM • AWS SDK de criptografia de banco de dados • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
Guias relacionados	Escolhendo serviços de AWS segurança, identidade e governança

Introdução

A criptografia é a base da segurança na computação em nuvem, ajudando a garantir a confidencialidade, integridade e autenticidade dos dados. Em um ambiente de nuvem, dados confidenciais podem atravessar redes públicas e residir em infraestrutura compartilhada, tornando essenciais medidas criptográficas robustas para proteção contra acesso não autorizado ou adulteração.

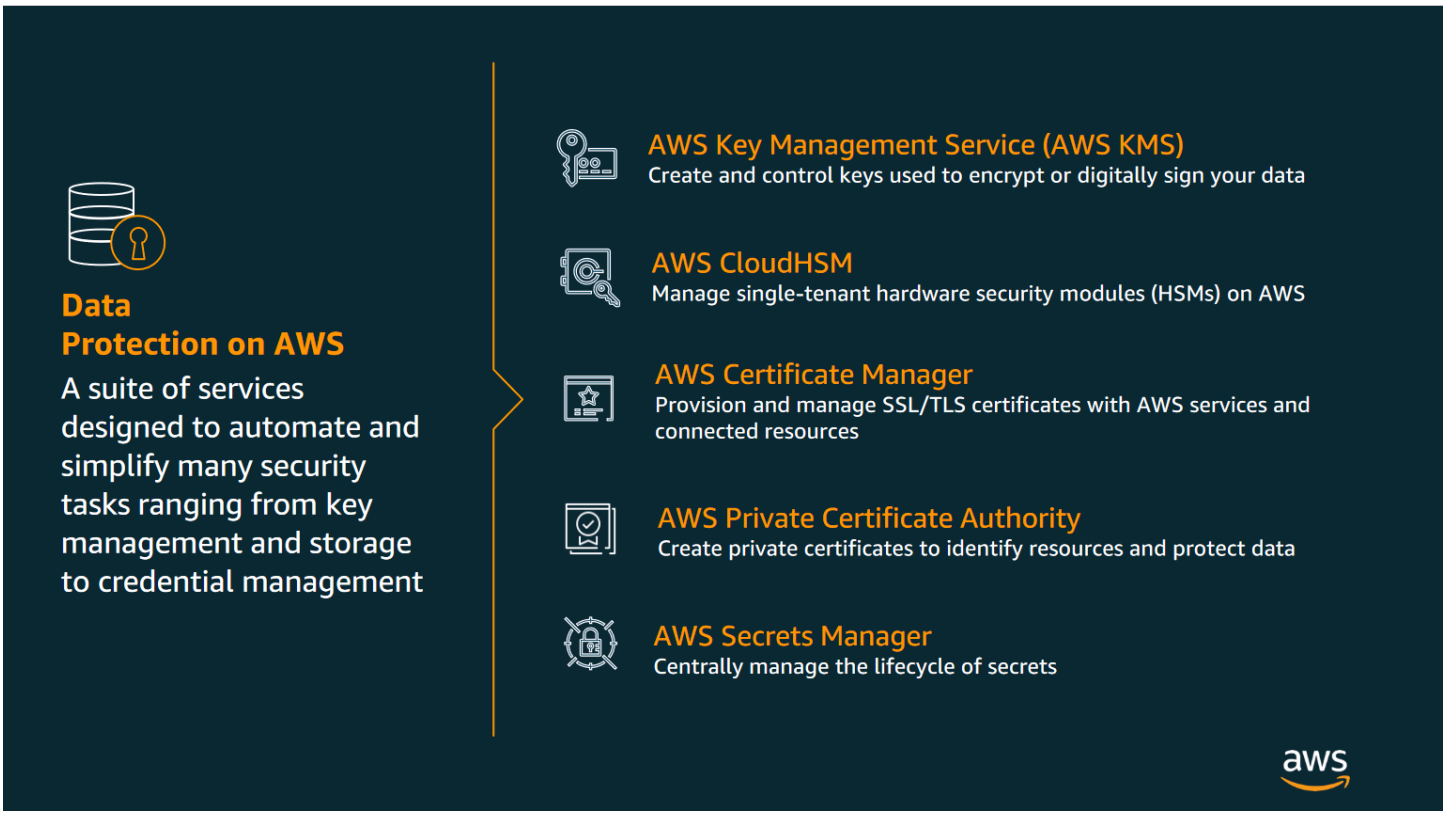
AWS oferece uma ampla variedade de serviços criptográficos para proteger dados, gerenciar chaves de criptografia e proteger informações confidenciais. Isso inclui AWS Key Management Service (KMS) para gerenciamento centralizado de chaves, AWS CloudHSM para PKCS11 aplicativos e módulos de segurança de hardware dedicados e AWS Encryption SDK para criptografia do lado do cliente. AWS Secrets Manager é um serviço que permite armazenar, gerenciar e recuperar com segurança informações confidenciais, como credenciais de banco de dados, chaves de API e outros

segredos, durante todo o ciclo de vida. AWS Certificate Manager (ACM) simplifica o processo de provisionamento, gerenciamento e implantação de certificados TLS (Transport Layer Security) publicamente confiáveis para uso com. Serviços da AWS O AWS Private Certificate Authority (PCA) permite gerar e distribuir certificados x509 para seus recursos internos.

O guia foi desenvolvido para ajudá-lo a escolher os serviços e ferramentas de AWS criptografia mais adequados às suas necessidades e à sua organização.

O vídeo a seguir é um segmento de dois minutos de uma apresentação que apresenta as melhores práticas para criptografia.

Compreendo



A escolha dos serviços de AWS criptografia certos depende do seu caso de uso específico, dos requisitos de segurança de dados, das obrigações de conformidade e das preferências operacionais, conforme descrito nas tabelas a seguir.

Key management

Se você precisar gerenciar com segurança as chaves de criptografia, considere o AWS Key Management Service (KMS). Ele permite que você crie, gire e gerencie chaves criptográficas

integradas com outras. Serviços da AWS O KMS usa a validação FIPS HSMs para ajudá-lo a atender aos requisitos de conformidade e fornecer garantia sobre a exatidão da implementação das primitivas criptográficas expostas pelo KMS. Alguns aplicativos exigem determinadas funções criptográficas ou interfaces de aplicativos que só estão disponíveis com um HSM tradicional e AWS CloudHSM fornecem módulos de segurança de hardware dedicados (HSMs) na nuvem, o que lhe dá controle total sobre suas chaves e operações criptográficas.

Data encryption

Para criptografar dados confidenciais, como detalhes do cliente ou propriedade intelectual, AWS KMS está totalmente integrado aos serviços de AWS armazenamento, banco de dados e mensagens (por exemplo, S3, RDS ou EBS). Se você precisar de criptografia do lado do cliente, AWS Encryption SDK é uma biblioteca de código aberto que facilita a criptografia de dados em seu aplicativo antes de enviá-los para a nuvem.

Secure communications

Para proteger os dados em trânsito, o AWS Certificate Manager (ACM) simplifica o gerenciamento de certificados TLS publicamente confiáveis. Use-o para afirmar a identidade de seus aplicativos voltados para a Internet e facilitar a comunicação criptografada entre seu aplicativo, usuários e serviços em nuvem sem se preocupar com renovações de certificados. Para aplicativos internos, você pode usar a Autoridade de Certificação AWS Privada (PCA) para gerar e distribuir certificados x509 para seus recursos internos, incluindo clientes e servidores.

Secrets and credentials management

Para armazenar e recuperar com segurança segredos de aplicativos, como credenciais de banco de dados, chaves de API ou certificados, considere. AWS Secrets Manager Ele fornece rotação secreta automatizada e controles de acesso refinados. Como alternativa, o AWS Systems Manager Parameter Store é uma opção de baixo custo para gerenciar configurações não confidenciais e pode ser integrado ao. AWS Secrets Manager

Compliance and auditing

Para o trabalho de conformidade regulamentar, considere AWS KMS e ajude AWS CloudHSM a garantir que os padrões de criptografia sejam atendidos. AWS O Artifact é um portal de autoatendimento que fornece acesso sob demanda aos relatórios AWS de segurança e conformidade, como certificações ISO e relatórios SOC, bem como a capacidade de revisar e aceitar acordos, como o Business Associate Addendum (BAA). Você também pode usar serviços como AWS Config, AWS Security Hub, e AWS Audit Manager para monitorar a conformidade e produzir os artefatos apropriados para seu próprio uso ou para consumo pelas partes interessadas.

Ao escolher entre serviços de AWS criptografia, considere os seguintes requisitos.

Requisito	Serviço
Baixo esforço, totalmente gerenciado	AWS KMS or AWS Secrets Manager
Exigir interfaces de aplicativos específicas ou algoritmos criptográficos não suportados pelo KMS	AWS CloudHSM
Encrypting/decrypting dados em seus aplicativos	AWS Encryption SDK
Gerenciamento simplificado de certificados TLS públicos	AWS Certificate Manager
Gerenciamento de segredos	AWS Secrets Manager

Ao alinhar seus requisitos com essas opções, você pode implementar soluções criptográficas adaptadas às suas necessidades operacionais e de segurança.

Considere

Escolher o serviço de AWS criptografia certo envolve entender suas necessidades específicas de segurança, operações e conformidade. AWS oferece uma variedade de serviços criptográficos, cada um projetado para lidar com diferentes casos de uso, desde gerenciamento de chaves até criptografia de dados e comunicação segura. Para tomar uma decisão informada, você deve avaliar seus requisitos com base em vários critérios críticos, incluindo seu caso de uso, necessidades de controle e flexibilidade, obrigações de conformidade, considerações de custo e integração com Serviços da AWS. Esses critérios ajudarão você a alinhar sua escolha às metas de segurança e aos fluxos de trabalho operacionais da sua organização.

Use case

Considere para que você precisa do serviço criptográfico: criptografia de dados, gerenciamento de chaves, comunicação segura ou gerenciamento de segredos. Por exemplo, AWS KMS é ideal para criptografia integrada Serviços da AWS, embora seja AWS CloudHSM adequado para organizações que precisam de determinados recursos criptográficos, interfaces de aplicativos

ou um HSM de inquilino único, geralmente devido à conformidade rigorosa ou às necessidades específicas de aplicativos. Esclarecer a finalidade garante que você selecione um serviço adequado às suas necessidades, otimizando tanto a funcionalidade quanto o custo.

Control and flexibility

Avalie o nível de controle necessário sobre suas operações criptográficas. Serviços gerenciados, como, AWS KMS fornecem facilidade de uso com o mínimo de sobrecarga de gerenciamento com um HSM multilocatário, mantendo controle total sobre seu material principal. Por outro lado, AWS CloudHSM oferece um modelo de inquilino único para necessidades específicas de aplicativos, criptografia ou conformidade.

Compliance requirements

Se você opera em um setor regulamentado, garanta que o serviço esteja alinhado com padrões como GDPR, PCI DSS ou HIPAA. AWS KMS e ambos AWS CloudHSM têm certificação FIPS 140-2 de nível 3. Selecionar um serviço que atenda aos seus requisitos não funcionais ajuda a manter a confiança e pode evitar possíveis penalidades legais ou financeiras.

Cost considerations

Avalie seu orçamento em relação ao modelo de preços do serviço. AWS KMS é econômico para as necessidades gerais de criptografia, ao mesmo tempo em que AWS CloudHSM incorre em custos mais altos devido ao hardware dedicado. Compreender as implicações de custo ajuda você a otimizar seus gastos com segurança.

Integration with AWS ecosystem

Se você usa muito Serviços da AWS, priorize uma solução de criptografia como o ACM que se integra perfeitamente ao S3, RDS AWS KMS ou Lambda. Isso garante fluxos de trabalho mais fluidos e reduz o esforço de desenvolvimento. Os recursos de integração podem aumentar significativamente a eficiência operacional.

Escolher

Escolher o serviço de AWS criptografia certo envolve entender suas necessidades específicas de segurança, operações e conformidade. AWS oferece uma variedade de serviços criptográficos, cada um projetado para lidar com diferentes casos de uso, desde gerenciamento de chaves até criptografia de dados e comunicação segura. Para tomar uma decisão informada, você deve avaliar seus requisitos com base em vários critérios críticos, incluindo seu caso de uso, necessidades de controle e flexibilidade, obrigações de conformidade, considerações de custo e integração com

Serviços da AWS. Esses critérios ajudarão você a alinhar sua escolha às metas de segurança e aos fluxos de trabalho operacionais da sua organização.

Caso de uso alvo	Quando você a usaria?	Serviço recomendado
Gerenciamento de chaves	Para criar, girar e gerenciar com segurança chaves criptográficas integradas com outros Serviços da AWS	AWS KMS
Gerenciamento de chaves	Para integrações específicas de aplicativos ou primitivas criptográficas	AWS CloudHSM
Criptografia de dados	Implementar a criptografia do lado do cliente para proteger dados confidenciais, como detalhes do cliente ou propriedade intelectual.	AWS Encryption SDK AWS SDK de criptografia de banco de dados
Comunicações seguras	Para proteger os dados em trânsito e simplificar o gerenciamento de SSL/TLS certificados.	AWS Certificate Manager AWS Private CA
Gerenciamento de segredos e credenciais	Para armazenar e recuperar com segurança segredos de aplicativos, como credenciais de banco de dados, chaves de API ou certificados.	AWS Secrets Manager AWS Parameter Store

Use

Agora você deve ter uma compreensão clara do que cada serviço de AWS criptografia faz e quais podem ser adequados para você.

Para explorar como usar e aprender mais sobre cada um dos serviços de AWS criptografia disponíveis, fornecemos um caminho para explorar como cada um deles funciona. As seções a

seguir fornecem links para documentação detalhada, tutoriais práticos e outros recursos para você começar.

AWS Certificate Manager

- Comece com AWS Certificate Manager

  Comece a usar AWS Certificate Manager, inclusive trabalhando com certificados públicos e privados.

  Explore o guia
- Melhores práticas para AWS Certificate Manager

  Analise as recomendações que podem ajudar você a usar com AWS Certificate Manager mais eficiência.

  Explore o guia
- AWS Certificate Manager PERGUNTAS FREQUENTES

  Consulte a página de perguntas frequentes AWS Certificate Manager (ACM) para obter respostas detalhadas a perguntas comuns sobre os recursos, capacidades e uso do ACM. Ele aborda tópicos como os tipos de certificados que o ACM gerencia, a integração com outros Serviços da AWS e orientações sobre provisionamento e gerenciamento de certificados. SSL/TLS

  Explore o FAQs

AWS CloudHSM

- Comece com AWS CloudHSM

  Saiba como criar, inicializar e ativar um cluster no AWS CloudHSM. Depois de concluir estes procedimentos, você estará pronto para gerenciar usuários e clusters, e usar as bibliotecas de software incluídas para executar operações de criptografia.

  Explore o guia
- Melhores práticas para AWS CloudHSM

  Explore as melhores práticas para gerenciar e monitorar seu AWS CloudHSM cluster.

Explore o guia

- AWS CloudHSM preços

  Consulte a página de preços para saber mais sobre AWS CloudHSM preços. Não há custos iniciais de uso do AWS CloudHSM. Com AWS CloudHSM, você paga uma taxa horária por cada HSM lançado até encerrar o HSM. Este guia fornece a taxa horária para cada AWS região.

  Explore a página de preços

- AWS CloudHSM PERGUNTAS FREQUENTES

  Consulte a página de perguntas AWS CloudHSM frequentes para obter respostas detalhadas a perguntas comuns sobre AWS CloudHSM, incluindo seus recursos, preços, provisionamento, segurança, conformidade, desempenho e integração com aplicativos de terceiros.

  Explore o FAQs

AWS Encryption SDK

- Comece com o AWS Encryption SDK

  Aprenda a usar o AWS Encryption SDK com AWS KMS.

  Explore o guia

- Melhores práticas para o AWS Encryption SDK

  Consulte a página de AWS Encryption SDK melhores práticas para obter orientação sobre como utilizá-las de forma eficaz AWS Encryption SDK para proteger seus dados. A adesão a essas melhores práticas ajuda a garantir a confidencialidade e a integridade de seus dados criptografados.

  Explore o guia

- AWS Encryption SDK PERGUNTAS FREQUENTES

  Consulte a página de perguntas AWS Encryption SDK frequentes para obter respostas a perguntas comuns sobre o AWS Encryption SDK, incluindo seus recursos, linguagens de programação suportadas e melhores práticas de implementação.

Explore as perguntas frequentes

AWS Database Encryption SDK

- Comece a usar o SDK AWS de criptografia de banco de dados

  Saiba como usar o SDK AWS de criptografia de banco de dados com o. AWS KMS

  Explore o guia
- Configurar o SDK AWS de criptografia de banco de dados

  Aprenda a configurar o SDK AWS de criptografia de banco de dados, incluindo a seleção de uma linguagem de programação e a seleção de chaves de encapsulamento.

  Explore o guia

AWS KMS

- Comece com AWS KMS

  Saiba como criar chaves KMS, incluindo chaves de criptografia simétricas e assimétricas.

  Explore o guia
- Melhores práticas para AWS KMS

  Aprenda as melhores práticas de criptografia para AWS KMS.

  Explore o guia
- AWS KMS preços

  Consulte a página de preços AWS Key Management Service (KMS) para saber mais sobre os custos associados ao uso AWS KMS, incluindo cobranças pelo armazenamento de chaves, solicitações de API e recursos opcionais, como armazenamentos de chaves personalizadas.

  Explore a página de preços
- AWS KMS PERGUNTAS FREQUENTES

  A página de perguntas frequentes AWS Key Management Service (KMS) fornece respostas detalhadas a perguntas comuns sobre AWS KMS, incluindo seus recursos, medidas de

segurança, práticas de cobrança, opções de gerenciamento de chaves e integração com outros. Serviços da AWS

Explore o FAQs

AWS Private CA

- Melhores práticas para AWS Private CA

  Analise as recomendações que podem ajudar você a usar AWS Private CA com eficiência.

  Explore o guia
- Comece com AWS Private CA

  Saiba como criar e ativar uma CA raiz programaticamente.

  Explore o guia
- AWS Private CA preços

  Analise os custos associados à operação privada CAs e à emissão de certificados privados.

  Explore a página de preços
- AWS Private CA PERGUNTAS FREQUENTES

  Obtenha respostas detalhadas para perguntas comuns sobre AWS Private CA, incluindo seus recursos, preços, provisionamento, segurança, conformidade, desempenho e integração com outros. Serviços da AWS

  Explore o FAQs

AWS Secrets Manager

- Comece com AWS Secrets Manager

  Saiba como criar um AWS Secrets Manager segredo.

  Explore o guia
- Melhores práticas para AWS Secrets Manager

  Conheça as melhores práticas que você deve considerar ao usar AWS Secrets Manager.

Explore o guia

- AWS Secrets Manager preços

  Consulte a página de AWS Secrets Manager preços para saber mais sobre os custos associados ao armazenamento, gerenciamento e recuperação seguros de segredos, como credenciais de banco de dados e chaves de API.

  Explore a página de preços

- AWS Secrets Manager PERGUNTAS FREQUENTES

  Consulte a página de perguntas AWS Secrets Manager frequentes para obter respostas detalhadas a perguntas comuns sobre AWS Secrets Manager, incluindo seus recursos, medidas de segurança, preços e recursos de integração.

  Explore o FAQs

Explore

- Pesquisa e recursos

  Explore AWS blogs, vídeos e ferramentas sobre criptografia.

  Revise os recursos

- Vídeos

  Assista a esses vídeos do canal AWS Developers YouTube para desenvolver e refinar ainda mais sua estratégia de criptografia.

  Explore vídeos sobre criptografia

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
Publicação inicial	Guia publicado pela primeira vez.	31 de janeiro de 2025

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.