AWS Guía de decisiones

Elegir un servicio de AWS criptografía

Elegir un servicio de AWS criptografía: AWS Guía de decisiones

Table of Contents

Guía de decisiones 1
Introducción 1
¿Entiende 2
Tenga en cuenta 4
Elija 6
Uso 7
Exploración 11
Historial del documento 13
..... xiv

Elegir un servicio de AWS criptografía

Dar el primer paso

Finalidad	Ayude a determinar qué servicios de AWS criptografía son los más adecuados para su organización.
Última actualización	31 de enero de 2025
Servicios cubiertos	• AWS Certificate Manager • AWS CloudHSM • AWS SDK de cifrado de bases de datos • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
Guías relacionadas	Elegir los servicios de AWS seguridad, identidad y gobierno

Introducción

La criptografía es una piedra angular de la seguridad en la computación en nube, ya que ayuda a garantizar la confidencialidad, integridad y autenticidad de los datos. En un entorno de nube, los datos confidenciales pueden atravesar las redes públicas y residir en una infraestructura compartida, lo que hace que las medidas criptográficas sólidas sean esenciales para protegerse contra el acceso no autorizado o la manipulación.

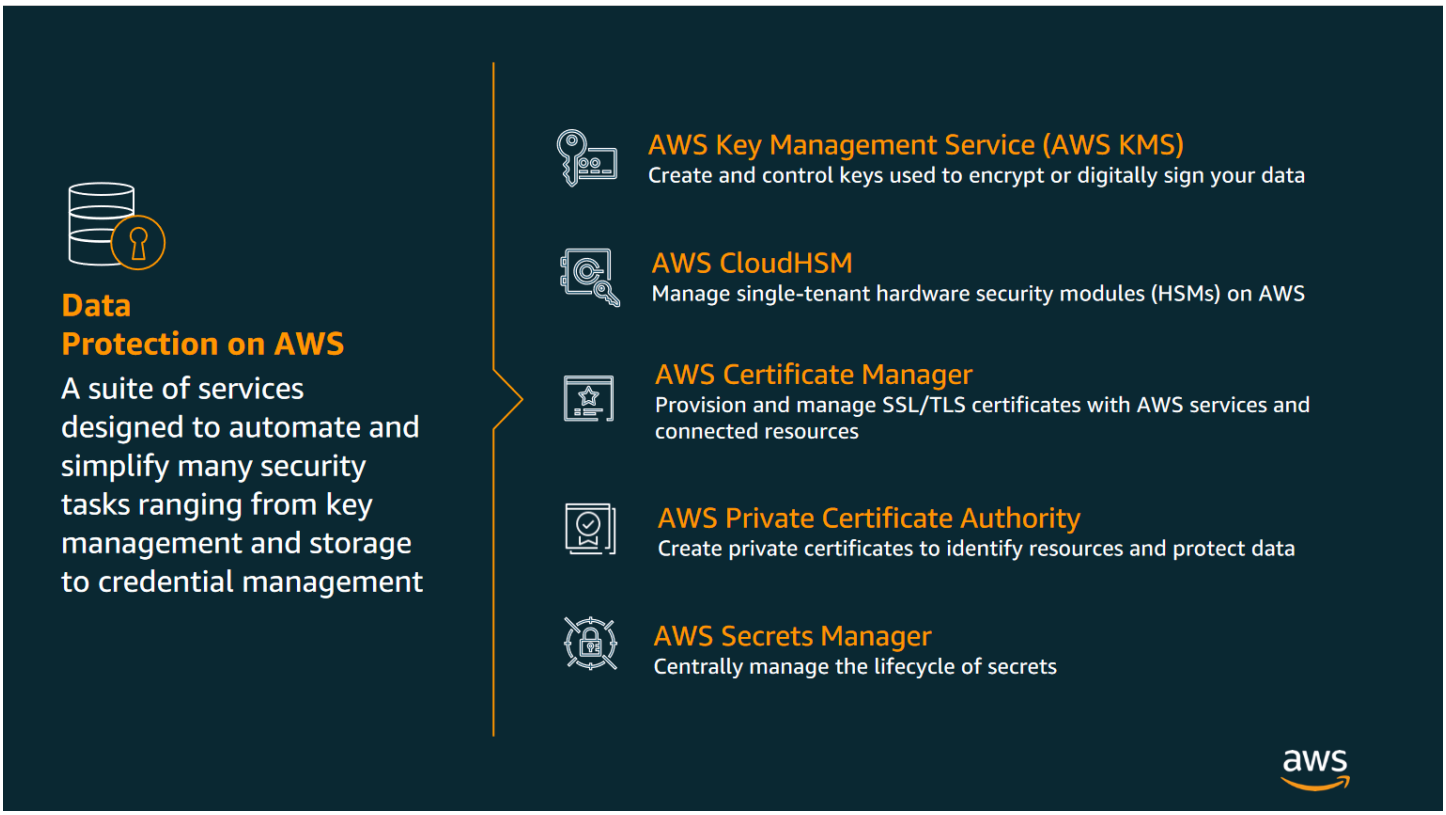
AWS ofrece una amplia gama de servicios criptográficos para proteger los datos, gestionar las claves de cifrado y proteger la información confidencial. Estos incluyen AWS Key Management Service (KMS) para la administración centralizada de claves, AWS CloudHSM para PKCS11 aplicaciones y módulos de seguridad de hardware dedicados, y AWS Encryption SDK para el cifrado del lado del cliente. AWS Secrets Manager es un servicio que le permite almacenar, gestionar y recuperar de forma segura información confidencial, como las credenciales de las bases de datos, las claves de

API y otros datos secretos, durante todo su ciclo de vida. AWS Certificate Manager (ACM) simplifica el proceso de aprovisionamiento, administración e implementación de certificados de seguridad de la capa de transporte (TLS) de confianza pública para su uso con. Servicios de AWS El AWS Private Certificate Authority (PCA) le permite generar y distribuir certificados x509 para sus recursos internos.

La guía está diseñada para ayudarle a elegir los servicios y herramientas de AWS criptografía que mejor se adapten a sus necesidades y a las de su organización.

El siguiente vídeo es un segmento de dos minutos de una presentación que presenta las mejores prácticas de criptografía.

¿Entiende



La elección de los servicios de AWS criptografía adecuados depende del caso de uso específico, de los requisitos de seguridad de los datos, de las obligaciones de cumplimiento y de las preferencias operativas, tal y como se indica en las siguientes tablas.

Key management

Si necesita administrar las claves de cifrado de forma segura, considere el Servicio de administración de AWS claves (KMS). Le permite crear, rotar y administrar claves criptográficas integradas con otras Servicios de AWS. KMS utiliza la validación FIPS HSMs para ayudarle a cumplir los requisitos de conformidad y garantizar la exactitud de la implementación de las primitivas criptográficas expuestas por KMS. Algunas aplicaciones requieren determinadas funciones criptográficas o interfaces de aplicación que solo están disponibles con un HSM tradicional y AWS CloudHSM proporcionan módulos de seguridad de hardware dedicados en la nube, lo que le permite tener un control total HSMs sobre sus claves y operaciones criptográficas.

Data encryption

Para cifrar datos confidenciales, como los datos de los clientes o la propiedad intelectual, AWS KMS está perfectamente integrado con los servicios de AWS almacenamiento, bases de datos y mensajería (por ejemplo, S3, RDS o EBS). Si necesita el cifrado del lado del cliente, AWS Encryption SDK se trata de una biblioteca de código abierto que facilita el cifrado de los datos de su aplicación antes de enviarlos a la nube.

Secure communications

Para proteger los datos en tránsito, AWS Certificate Manager (ACM) simplifica la administración de los certificados TLS de confianza pública. Úselo para confirmar la identidad de sus aplicaciones conectadas a Internet y facilitar el cifrado de las comunicaciones entre su aplicación, los usuarios y los servicios en la nube sin tener que preocuparse por la renovación de los certificados. En el caso de las aplicaciones internas, puede utilizar una autoridad de certificación AWS privada (PCA) para generar y distribuir certificados x509 para sus recursos internos, incluidos los clientes y los servidores.

Secrets and credentials management

Para almacenar y recuperar de forma segura los secretos de las aplicaciones, como las credenciales de las bases de datos, las claves de API o los certificados, considere la posibilidad de hacerlo. AWS Secrets Manager Proporciona una rotación automática de secretos y controles de acceso detallados. Como alternativa, AWS Systems Manager Parameter Store es una opción de menor costo para administrar configuraciones no confidenciales y se puede integrar con. AWS Secrets Manager

Compliance and auditing

Para la labor de conformidad normativa, considere AWS KMS y ayude AWS CloudHSM a garantizar el cumplimiento de los estándares de cifrado. AWS Artifact es un portal de autoservicio

que proporciona acceso bajo demanda a los informes AWS de seguridad y cumplimiento, como las certificaciones ISO y los informes SOC, así como la posibilidad de revisar y aceptar acuerdos como el Business Associate Addendum (BAA). También puede utilizar servicios como AWS Config y supervisar el cumplimiento y AWS Audit Manager producir los artefactos adecuados para su propio uso o para que los consuman las partes interesadas. AWS Security Hub

Al elegir entre los servicios de AWS criptografía, tenga en cuenta los siguientes requisitos.

Requisito	Servicio
Bajo esfuerzo, totalmente gestionado	AWS KMS o bien AWS Secrets Manager
Requieren interfaces de aplicación o algoritmos criptográficos específicos que KMS no admite	AWS CloudHSM
Encrypting/decrypting datos en sus aplicacio nes	AWS Encryption SDK
Administración simplificada de certificados TLS públicos	AWS Certificate Manager
Administración de secretos	AWS Secrets Manager

Al alinear sus requisitos con estas opciones, puede implementar soluciones criptográficas adaptadas a sus necesidades operativas y de seguridad.

Tenga en cuenta

Elegir el servicio de AWS criptografía adecuado implica comprender sus necesidades específicas de seguridad, operativas y de cumplimiento. AWS ofrece una variedad de servicios criptográficos, cada uno diseñado para abordar diferentes casos de uso, desde la administración de claves hasta el cifrado de datos y la comunicación segura. Para tomar una decisión informada, debe evaluar sus requisitos en función de varios criterios fundamentales, incluidos su caso de uso, sus necesidades de control y flexibilidad, las obligaciones de cumplimiento, las consideraciones de costo y la integración con Servicios de AWS ellos. Estos criterios le ayudarán a alinear su elección con los objetivos de seguridad y los flujos de trabajo operativos de su organización.

Use case

Considere para qué necesita el servicio criptográfico: cifrado de datos, administración de claves, comunicación segura o administración de secretos. Por ejemplo, AWS KMS es ideal para integrar el cifrado y, al mismo tiempo Servicios de AWS, AWS CloudHSM se adapta a las organizaciones que necesitan determinadas capacidades criptográficas, interfaces de aplicaciones o un HSM de un solo usuario, a menudo debido a un cumplimiento estricto o a necesidades específicas de las aplicaciones. Al aclarar el propósito, se garantiza la selección de un servicio adecuado a sus necesidades, lo que optimiza tanto la funcionalidad como el costo.

Control and flexibility

Evalúe el nivel de control que necesita sobre sus operaciones criptográficas. Los servicios gestionados, como AWS KMS este, proporcionan facilidad de uso con una sobrecarga de administración mínima con un HSM multiusuario y, al mismo tiempo, mantienen el control total sobre el material clave. Por el contrario, AWS CloudHSM ofrece un modelo de inquilino único para necesidades específicas de aplicación, criptografía o cumplimiento.

Compliance requirements

Si opera en un sector regulado, asegúrese de que el servicio cumpla con estándares como el GDPR, el PCI DSS o la HIPAA. AWS KMS y ambos AWS CloudHSM cuentan con la certificación FIPS 140-2 de nivel 3. La selección de un servicio que cumpla con sus requisitos no funcionales ayuda a mantener la confianza y puede evitar posibles sanciones legales o financieras.

Cost considerations

Evalúe su presupuesto en función del modelo de precios del servicio. AWS KMS es rentable para las necesidades generales de cifrado, mientras que AWS CloudHSM incurre en costes más altos debido al hardware dedicado. Comprender las implicaciones en materia de costes le ayuda a optimizar sus gastos de seguridad.

Integration with AWS ecosystem

Si lo usa mucho Servicios de AWS, priorice una solución de criptografía como AWS KMS ACM que se integre perfectamente con S3, RDS o Lambda. Esto garantiza flujos de trabajo más fluidos y reduce el esfuerzo de desarrollo. Las capacidades de integración pueden mejorar significativamente la eficiencia operativa.

Elija

Elegir el servicio de AWS criptografía adecuado implica comprender sus necesidades específicas de seguridad, operativas y de cumplimiento. AWS ofrece una variedad de servicios criptográficos, cada uno diseñado para abordar diferentes casos de uso, desde la administración de claves hasta el cifrado de datos y la comunicación segura. Para tomar una decisión informada, debe evaluar sus requisitos en función de varios criterios fundamentales, incluidos su caso de uso, sus necesidades de control y flexibilidad, las obligaciones de cumplimiento, las consideraciones de costo y la integración con Servicios de AWS ellos. Estos criterios le ayudarán a alinear su elección con los objetivos de seguridad y los flujos de trabajo operativos de su organización.

Caso de uso objetivo	¿Cuándo lo usaría?	Servicio recomendado
Administración de claves	Para crear, rotar y administrar de forma segura claves criptográficas integradas con otras Servicios de AWS	AWS KMS
Administración de claves	Para integraciones de aplicaciones específicas o primitivas criptográficas	AWS CloudHSM
Cifrado de datos	Implementar el cifrado del lado del cliente para proteger los datos confidenciales, como los detalles de los clientes o la propiedad intelectual.	AWS Encryption SDK AWS SDK de cifrado de bases de datos
Comunicaciones seguras	Para proteger los datos en tránsito y simplificar la administración de SSL/TLS los certificados.	AWS Certificate Manager AWS Private CA
Gestión de secretos y credenciales	Para almacenar y recuperar de forma segura los secretos de las aplicaciones, como las credenciales de la base de	AWS Secrets Manager AWS Parameter Store

Caso de uso objetivo	¿Cuándo lo usaría?	Servicio recomendado
	datos, las claves de API o los certificados.	

Uso

Ahora debería tener una idea clara de lo que hace cada servicio de AWS criptografía y cuáles podrían ser adecuados para usted.

Para explorar cómo usar cada uno de los servicios de AWS criptografía disponibles y obtener más información sobre ellos, hemos proporcionado una vía para explorar cómo funciona cada uno de ellos. Las siguientes secciones proporcionan enlaces a documentación detallada, tutoriales prácticos y otros recursos para que pueda empezar.

AWS Certificate Manager

- Comience con AWS Certificate Manager

  Comience a usarlos AWS Certificate Manager, incluso a trabajar con certificados públicos y privados.

  Exploración de la guía
- Prácticas recomendadas para AWS Certificate Manager

  Revise las recomendaciones que pueden ayudarle a utilizarlas de forma AWS Certificate Manager más eficaz.

  Exploración de la guía
- AWS Certificate Manager Preguntas frecuentes

  Consulte la página de preguntas frecuentes AWS Certificate Manager (ACM) para obtener respuestas detalladas a las preguntas más frecuentes sobre las funciones, las capacidades y el uso de ACM. Abarca temas como los tipos de certificados que gestiona ACM, la integración con otros Servicios de AWS certificados y las directrices sobre el aprovisionamiento y la administración de los certificados. SSL/TLS

  Explore las FAQs

AWS CloudHSM

- Comience con AWS CloudHSM

  Aprenda a crear, inicializar y activar un clúster en AWS CloudHSM. Después de completar estos procedimientos, estará preparado para administrar usuarios y clústeres, y para utilizar las bibliotecas de software incluidas para realizar operaciones criptográficas.

  Exploración de la guía

- Prácticas recomendadas para AWS CloudHSM

  Explore las mejores prácticas para administrar y monitorear su AWS CloudHSM clúster.

  Exploración de la guía

- AWS CloudHSM precios

  Consulta la página de precios para obtener más información sobre AWS CloudHSM los precios. Su uso de AWS CloudHSM no conlleva costos iniciales. Con AWS CloudHSM, pagas una tarifa por hora por cada HSM que lances hasta que canceles el HSM. Esta guía proporciona la tarifa por hora para cada AWS región.

  Explora la página de precios

- AWS CloudHSM Preguntas frecuentes

  Consulta la página de AWS CloudHSM preguntas frecuentes para obtener respuestas detalladas a las preguntas más frecuentes sobre AWS CloudHSM sus funciones, precios, aprovisionamiento, seguridad, conformidad, rendimiento e integración con aplicaciones de terceros.

  Explore las FAQs

AWS Encryption SDK

- Comience con el AWS Encryption SDK

  Aprenda a usar el AWS Encryption SDK con AWS KMS.

  Exploración de la guía

- Mejores prácticas para AWS Encryption SDK

Consulte la página de AWS Encryption SDK mejores prácticas para obtener orientación sobre cómo utilizarlas de forma eficaz AWS Encryption SDK para proteger sus datos. El cumplimiento de estas mejores prácticas ayuda a garantizar la confidencialidad e integridad de sus datos cifrados.

Exploración de la guía

- AWS Encryption SDK PREGUNTAS FRECUENTES

  Consulte la página de AWS Encryption SDK preguntas frecuentes para obtener respuestas a las preguntas más frecuentes sobre AWS Encryption SDK, incluidas sus características, los lenguajes de programación compatibles y las mejores prácticas de implementación.

  Explore las preguntas frecuentes

AWS Database Encryption SDK

- Comience con el SDK de cifrado AWS de bases de datos

  Aprenda a usar el SDK de cifrado AWS de bases de datos con AWS KMS.

  Exploración de la guía

- Configure el SDK AWS de cifrado de bases de datos

  Aprenda a configurar el SDK de cifrado de AWS bases de datos, incluida la selección de un lenguaje de programación y la selección de las claves de empaquetado.

  Exploración de la guía

AWS KMS

- Comience con AWS KMS

  Aprenda a crear claves KMS, incluidas claves de cifrado simétricas y asimétricas.

  Exploración de la guía

- Prácticas recomendadas para AWS KMS

  Conozca las mejores prácticas de cifrado para AWS KMS.

Exploración de la guía

- AWS KMS precios

  Consulta la página de precios AWS Key Management Service (KMS) para obtener información sobre los costes asociados al uso AWS KMS, incluidos los cargos por el almacenamiento de claves, las solicitudes de API y las funciones opcionales, como los almacenes de claves personalizados.

  Consulta la página de precios

- AWS KMS Preguntas frecuentes

  La página de preguntas frecuentes de AWS Key Management Service (KMS) proporciona respuestas detalladas a preguntas frecuentes sobre AWS KMS sus funciones, medidas de seguridad, prácticas de facturación, opciones de administración de claves e integración con otras Servicios de AWS.

  Explore las FAQs

AWS Private CA

- Mejores prácticas para AWS Private CA

  Revise las recomendaciones que pueden ayudarle a utilizarlas de AWS Private CA forma eficaz.

  Exploración de la guía

- Comience con AWS Private CA

  Aprenda a crear y activar una CA raíz mediante programación.

  Exploración de la guía

- AWS Private CA precios

  Revise los costos asociados con la operación privada CAs y la emisión de certificados privados.

  Explore la página de precios

- AWS Private CA Preguntas frecuentes

Obtenga respuestas detalladas a las preguntas más frecuentes sobre AWS Private CA sus funciones, precios, aprovisionamiento, seguridad, conformidad, rendimiento e integración con otras Servicios de AWS.

Explore las FAQs

AWS Secrets Manager

- Comience con AWS Secrets Manager

  Aprenda a crear un AWS Secrets Manager secreto.

  Exploración de la guía
- Mejores prácticas para AWS Secrets Manager

  Conozca las prácticas recomendadas que debe tener en cuenta a la hora de utilizarlas AWS Secrets Manager.

  Exploración de la guía
- AWS Secrets Manager precios

  Consulta la página de AWS Secrets Manager precios para obtener información sobre los costes asociados al almacenamiento, la gestión y la recuperación de datos confidenciales de forma segura, como las credenciales de las bases de datos y las claves de API.

  Explore la página de precios
- AWS Secrets Manager Preguntas frecuentes

  Consulta la página de AWS Secrets Manager preguntas frecuentes para obtener respuestas detalladas a las preguntas más frecuentes sobre AWS Secrets Manager sus funciones, medidas de seguridad, precios y capacidades de integración.

  Explore las FAQs

Exploración

- Investigación y recursos

Explore AWS blogs, vídeos y herramientas sobre criptografía.

Revise los recursos

- Videos

  Vea estos vídeos del canal de AWS desarrolladores YouTube para seguir desarrollando y perfeccionando su estrategia de criptografía.

  Explore los vídeos de criptografía

Historial del documento

En la siguiente tabla se describen los cambios importantes en esta guía de decisiones. Para recibir notificaciones sobre las actualizaciones de esta guía, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Publicación inicial	La guía se publicó por primera vez.	31 de enero de 2025

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.