AWS Guida decisionale

Scelta di un AWS servizio di crittografia

Scelta di un AWS servizio di crittografia: AWS Guida decisionale

Table of Contents

Scelta di un AWS servizio di crittografia

Fare il primo passo

Scopo	Aiutaci a determinare quali servizi di AWS crittografia sono più adatti alla tua organizza zione.
Ultimo aggiornamento	31 gennaio 2025
Servizi coperti	• AWS Certificate Manager • AWS CloudHSM • AWS SDK per la crittografia del database • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
Guide correlate	Scelta AWS dei servizi di sicurezza, identità e governance

Introduzione

La crittografia è una pietra miliare della sicurezza nel cloud computing, poiché aiuta a garantire la riservatezza, l'integrità e l'autenticità dei dati. In un ambiente cloud, i dati sensibili possono attraversare reti pubbliche e risiedere su infrastrutture condivise, il che rende essenziali solide misure crittografiche per la protezione da accessi non autorizzati o manomissioni.

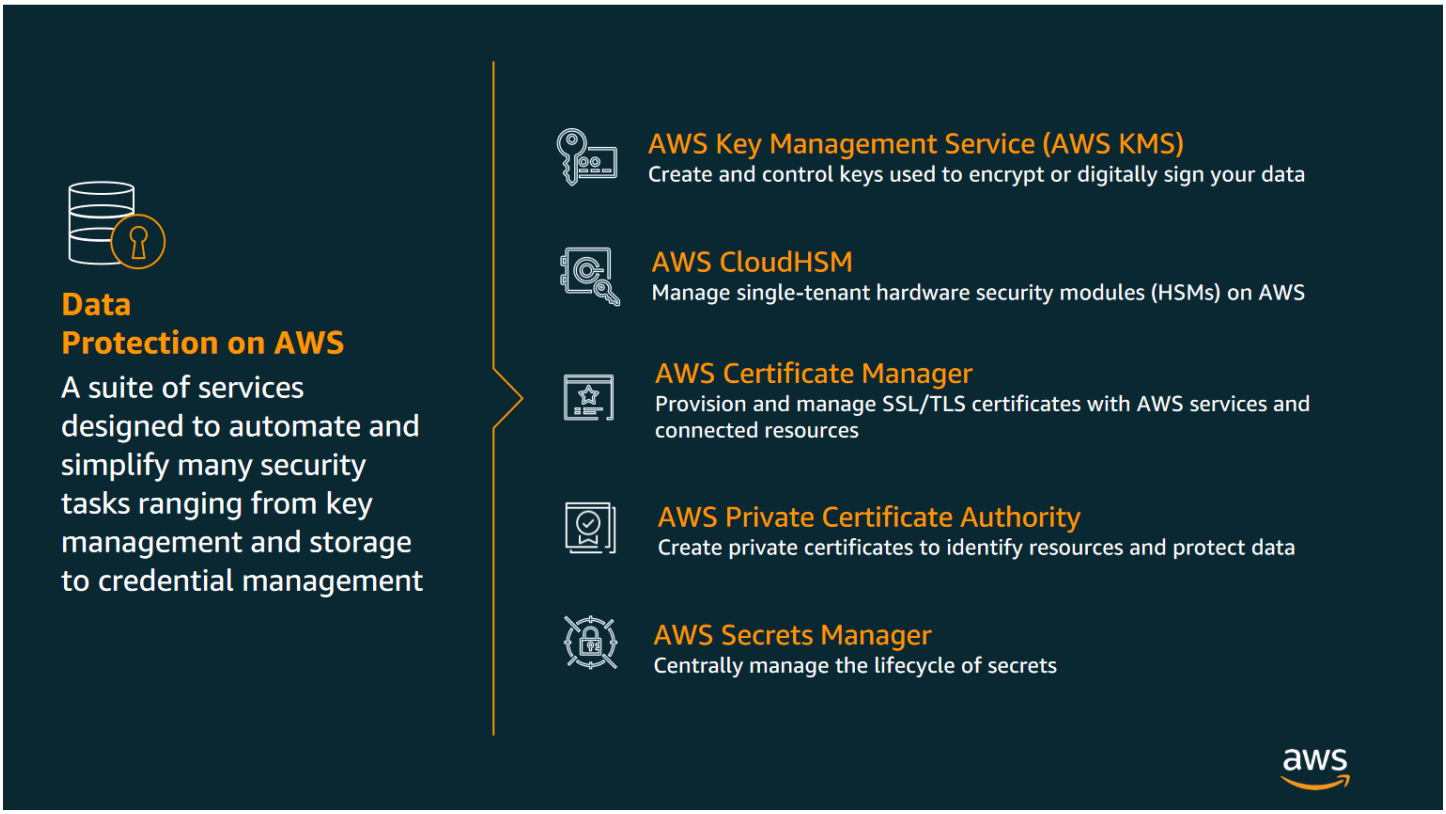
AWS offre una gamma completa di servizi crittografici per proteggere i dati, gestire le chiavi di crittografia e proteggere le informazioni sensibili. Questi includono AWS Key Management Service (KMS) per la gestione centralizzata delle chiavi, AWS CloudHSM per PKCS11 applicazioni e moduli di sicurezza hardware dedicati e AWS Encryption SDK per la crittografia lato client. AWS Secrets Manager è un servizio che consente di archiviare, gestire e recuperare in modo sicuro informazioni sensibili come credenziali di database, chiavi API e altri segreti durante tutto il loro ciclo di vita. AWS Certificate Manager (ACM) semplifica il processo di fornitura, gestione e distribuzione di certificati

TLS (Transport Layer Security) pubblicamente affidabili da utilizzare con. Servizi AWS Il AWS Private Certificate Authority (PCA) consente di generare e distribuire certificati x509 per le risorse interne.

La guida è progettata per aiutarvi a scegliere i servizi e gli strumenti di AWS crittografia più adatti alle vostre esigenze e alla vostra organizzazione.

Il video seguente è un segmento di due minuti di una presentazione che introduce le migliori pratiche per la crittografia.

Comprendi



La scelta dei servizi di AWS crittografia giusti dipende dal caso d'uso specifico, dai requisiti di sicurezza dei dati, dagli obblighi di conformità e dalle preferenze operative, come indicato nelle tabelle seguenti.

Key management

Se hai bisogno di gestire in modo sicuro le chiavi di crittografia, prendi in considerazione AWS Key Management Service (KMS). Consente di creare, ruotare e gestire chiavi crittografiche integrate con altre. Servizi AWS KMS utilizza la certificazione FIPS HSMs per aiutarvi a soddisfare i requisiti di conformità e per fornire garanzie sulla correttezza dell'implementazione delle primitive

crittografiche esposte da KMS. Alcune applicazioni richiedono determinate funzioni crittografiche o interfacce applicative che sono disponibili solo con un HSM tradizionale e forniscono moduli di sicurezza hardware dedicati () nel cloud che AWS CloudHSM offrono il pieno controllo sulle chiavi e sulle operazioni crittografiche. HSMs

Data encryption

Per crittografare dati sensibili come i dati dei clienti o la proprietà intellettuale, AWS KMS è strettamente integrato con i servizi di AWS archiviazione, database e messaggistica (ad esempio S3, RDS o EBS). Se hai bisogno della crittografia lato client, AWS Encryption SDK è una libreria open source che semplifica la crittografia dei dati all'interno dell'applicazione prima di inviarli al cloud.

Secure communications

Per proteggere i dati in transito, AWS Certificate Manager (ACM) semplifica la gestione dei certificati TLS pubblicamente affidabili. Usalo per affermare l'identità delle tue applicazioni con accesso a Internet e facilitare la crittografia delle comunicazioni tra l'applicazione, gli utenti e i servizi cloud senza preoccuparti del rinnovo dei certificati. Per le applicazioni interne, è possibile utilizzare AWS Private Certificate Authority (PCA) per generare e distribuire certificati x509 per le risorse interne, inclusi client e server.

Secrets and credentials management

Per archiviare e recuperare in modo sicuro i segreti delle applicazioni come le credenziali del database, le chiavi API o i certificati, prendi in considerazione. AWS Secrets Manager Fornisce una rotazione segreta automatizzata e controlli di accesso dettagliati. In alternativa, AWS Systems Manager Parameter Store è un'opzione a basso costo per la gestione di configurazioni non sensibili e può essere integrata con. AWS Secrets Manager

Compliance and auditing

Per quanto riguarda la conformità normativa, prendete in considerazione AWS KMS e contribuite AWS CloudHSM a garantire il rispetto degli standard di crittografia. AWS Artifact è un portale self-service che fornisce l'accesso su richiesta AWS ai report di sicurezza e conformità, come le certificazioni ISO e i report SOC, oltre alla possibilità di rivedere e accettare accordi come il Business Associate Addendum (BAA). Puoi anche utilizzare servizi come AWS Config e monitorare la conformità e AWS Audit Manager produrre gli artefatti appropriati per il tuo uso o per il consumo da parte delle parti interessate. AWS Security Hub

Quando scegli tra i servizi di AWS crittografia, considera i seguenti requisiti.

Requisito	Servizio
Sforzo ridotto, gestione completa	AWS KMS oppure AWS Secrets Manager
Richiedono interfacce applicative specifiche o algoritmi crittografici non supportati da KMS	AWS CloudHSM
Encrypting/decrypting dati nelle tue applicazioni	AWS Encryption SDK
Gestione semplificata dei certificati TLS pubblici	AWS Certificate Manager
Gestione dei segreti	AWS Secrets Manager

Allineando i requisiti a queste opzioni, è possibile implementare soluzioni crittografiche personalizzate in base alle esigenze operative e di sicurezza.

Considera

La scelta del servizio di AWS crittografia giusto implica la comprensione delle esigenze specifiche di sicurezza, operative e conformità. AWS offre una varietà di servizi crittografici, ciascuno progettato per soddisfare diversi casi d'uso, dalla gestione delle chiavi alla crittografia dei dati e alla comunicazione sicura. Per prendere una decisione informata, è necessario valutare i requisiti in base a diversi criteri critici, tra cui il caso d'uso, le esigenze di controllo e flessibilità, gli obblighi di conformità, le considerazioni sui costi e l'integrazione con. Servizi AWS Questi criteri vi aiuteranno ad allineare la vostra scelta agli obiettivi di sicurezza e ai flussi di lavoro operativi della vostra organizzazione.

Use case

Considerate a cosa vi serve il servizio di crittografia: crittografia dei dati, gestione delle chiavi, comunicazioni sicure o gestione dei segreti. Ad esempio, AWS KMS è ideale per la crittografia integrata in Servizi AWS, mentre è AWS CloudHSM adatto alle organizzazioni che necessitano di determinate funzionalità crittografiche, interfacce applicative o un HSM a tenant singolo, spesso a causa di una conformità rigorosa o di esigenze applicative specifiche. Chiarendo lo scopo è possibile selezionare un servizio adatto alle proprie esigenze, ottimizzando funzionalità e costi.

Control and flexibility

Valuta il livello di controllo di cui hai bisogno sulle tue operazioni crittografiche. I servizi gestiti, ad esempio, AWS KMS offrono facilità d'uso con un sovraccarico di gestione minimo con un HSM multi-tenant, pur mantenendo il pieno controllo sul materiale chiave. Al contrario, AWS CloudHSM offre un modello single-tenant per esigenze applicative, crittografiche o di conformità specifiche.

Compliance requirements

Se operi in un settore regolamentato, assicurati che il servizio sia in linea con standard come GDPR, PCI DSS o HIPAA. AWS KMS e AWS CloudHSM sono entrambi certificati FIPS 140-2 di livello 3. La scelta di un servizio che soddisfi i requisiti non funzionali aiuta a mantenere la fiducia e può evitare potenziali sanzioni legali o finanziarie.

Cost considerations

Valuta il tuo budget rispetto al modello di prezzo del servizio. AWS KMS è conveniente per le esigenze generali di crittografia, mentre AWS CloudHSM comporta costi più elevati grazie all'hardware dedicato. La comprensione delle implicazioni in termini di costi aiuta a ottimizzare le spese per la sicurezza.

Integration with AWS ecosystem

Se ne usi molto Servizi AWS, dai la priorità a una soluzione di crittografia come AWS KMS o ACM che si integra perfettamente con S3, RDS o Lambda. Ciò garantisce flussi di lavoro più fluidi e riduce lo sforzo di sviluppo. Le funzionalità di integrazione possono migliorare in modo significativo l'efficienza operativa.

Scegliere

La scelta del servizio di AWS crittografia giusto implica la comprensione delle esigenze specifiche di sicurezza, operative e conformità. AWS offre una varietà di servizi crittografici, ciascuno progettato per soddisfare diversi casi d'uso, dalla gestione delle chiavi alla crittografia dei dati e alla comunicazione sicura. Per prendere una decisione informata, è necessario valutare i requisiti in base a diversi criteri critici, tra cui il caso d'uso, le esigenze di controllo e flessibilità, gli obblighi di conformità, le considerazioni sui costi e l'integrazione con. Servizi AWS Questi criteri vi aiuteranno ad allineare la vostra scelta agli obiettivi di sicurezza e ai flussi di lavoro operativi della vostra organizzazione.

Caso d'uso target	Quando lo useresti?	Servizio consigliato
Gestione delle chiavi	Per creare, ruotare e gestire in modo sicuro chiavi crittografiche integrate con altre Servizi AWS	AWS KMS
Gestione delle chiavi	Per integrazioni di applicazioni specifiche o primitive crittografiche	AWS CloudHSM
Crittografia dei dati	Implementare la crittografia lato client per proteggere dati sensibili come i dettagli dei clienti o la proprietà intellettuale.	AWS Encryption SDK AWS SDK per la crittografia del database
Sicurezza delle comunicazioni	Per proteggere i dati in transito e semplificare la gestione dei SSL/TLS certificati.	AWS Certificate Manager AWS Private CA
Gestione dei segreti e delle credenziali	Per archiviare e recuperare in modo sicuro i segreti delle applicazioni come credenziali del database, chiavi API o certificati.	AWS Secrets Manager AWS Archivio dei parametri

Utilizzo

Ora dovresti avere una chiara comprensione di ciò che fa ogni servizio di AWS crittografia e quali potrebbero essere quelli giusti per te.

Per scoprire come utilizzare e saperne di più su ciascuno dei servizi di AWS crittografia disponibili, abbiamo fornito un percorso per scoprire come funziona ciascuno di essi. Le sezioni seguenti forniscono collegamenti a documentazione approfondita, tutorial pratici e altre risorse per iniziare.

AWS Certificate Manager

- Inizia con AWS Certificate Manager

  Inizia a utilizzare AWS Certificate Manager, incluso l'utilizzo di certificati pubblici e privati.

  Esplora la guida
- Le migliori pratiche per AWS Certificate Manager

  Consulta i consigli che possono aiutarti a utilizzare in modo AWS Certificate Manager più efficace.

  Esplora la guida
- AWS Certificate Manager Domande frequenti

  Consulta la pagina delle domande frequenti AWS Certificate Manager (ACM) per risposte dettagliate alle domande più comuni sulle caratteristiche, le funzionalità e l'utilizzo di ACM. Tratta argomenti come i tipi di certificati gestiti da ACM, l'integrazione con altri Servizi AWS e le linee guida sul provisioning e la gestione dei certificati. SSL/TLS

  Esplora il FAQs

AWS CloudHSM

- Inizia con AWS CloudHSM

  Scopri come creare, inizializzare e attivare un cluster in AWS CloudHSM. Dopo aver completato queste procedure, sarai pronto a gestire gli utenti e i cluster, nonché a eseguire operazioni di crittografia utilizzando le librerie software in dotazione.

  Esplora la guida
- Le migliori pratiche per AWS CloudHSM

  Esplora le best practice per la gestione e il monitoraggio AWS CloudHSM del cluster.

  Esplora la guida
- AWS CloudHSM prezzi

  Consulta la pagina dei prezzi per maggiori informazioni sui AWS CloudHSM prezzi. Non sono previsti costi iniziali per l'utilizzo AWS CloudHSM. Con AWS CloudHSM, paghi una tariffa oraria

per ogni HSM avviato fino alla chiusura dell'HSM. Questa guida fornisce la tariffa oraria per ogni regione. AWS

Esplora la pagina dei prezzi

- AWS CloudHSM Domande frequenti

  AWS CloudHSM Consulta la pagina delle domande frequenti per risposte dettagliate alle domande più frequenti AWS CloudHSM, tra cui funzionalità, prezzi, provisioning, sicurezza, conformità, prestazioni e integrazione con applicazioni di terze parti.

  Esplora il FAQs

AWS Encryption SDK

- Inizia con AWS Encryption SDK

  Scopri come usare AWS Encryption SDK il AWS KMS.

  Esplora la guida

- Le migliori pratiche per AWS Encryption SDK

  Consulta la pagina AWS Encryption SDK Best Practices per indicazioni su come utilizzarle in modo efficace AWS Encryption SDK per proteggere i tuoi dati. L'adesione a queste best practice aiuta a garantire la riservatezza e l'integrità dei dati crittografati.

  Esplora la guida

- AWS Encryption SDK Domande frequenti

  AWS Encryption SDK Consulta la pagina delle domande frequenti per le risposte alle domande più comuni su AWS Encryption SDK, comprese le funzionalità, i linguaggi di programmazione supportati e le migliori pratiche per l'implementazione.

  Esplora le domande frequenti

AWS Database Encryption SDK

- Inizia a usare AWS Database Encryption SDK

  Scopri come utilizzare AWS Database Encryption SDK con. AWS KMS

Esplora la guida

- Configura il AWS Database Encryption SDK

  Scopri come configurare il AWS Database Encryption SDK, inclusa la selezione di un linguaggio di programmazione e la selezione delle chiavi di wrapping.

  Esplora la guida

AWS KMS

- Inizia con AWS KMS

  Scopri come creare chiavi KMS, incluse chiavi di crittografia simmetriche e asimmetriche.

  Esplora la guida

- Le migliori pratiche per AWS KMS

  Scopri le migliori pratiche di crittografia per AWS KMS.

  Esplora la guida

- AWS KMS prezzi

  Consulta la pagina dei prezzi di AWS Key Management Service (KMS) per scoprire i costi associati all'utilizzo AWS KMS, inclusi i costi per l'archiviazione delle chiavi, le richieste API e le funzionalità opzionali come gli archivi di chiavi personalizzati.

  Esplora la pagina dei prezzi

- AWS KMS Domande frequenti

  La pagina delle domande frequenti su AWS Key Management Service (KMS) fornisce risposte dettagliate alle domande più comuni AWS KMS, tra cui le funzionalità, le misure di sicurezza, le pratiche di fatturazione, le opzioni di gestione delle chiavi e l'integrazione con altre. Servizi AWS

  Esplora il FAQs

AWS Private CA

- Le migliori pratiche per AWS Private CA

Consulta i consigli che possono aiutarti a utilizzare AWS Private CA in modo efficace.

Esplora la guida

- Inizia con AWS Private CA

  Scopri come creare e attivare una CA root a livello di codice.

  Esplora la guida

- AWS Private CA prezzi

  Esamina i costi associati alla gestione privata CAs e all'emissione di certificati privati.

  Esplora la pagina dei prezzi

- AWS Private CA Domande frequenti

  Ottieni risposte dettagliate alle domande più frequenti AWS Private CA, tra cui funzionalità, prezzi, approvvigionamento, sicurezza, conformità, prestazioni e integrazione con altri Servizi AWS.

  Esplora il FAQs

AWS Secrets Manager

- Inizia con AWS Secrets Manager

  Scopri come creare un AWS Secrets Manager segreto.

  Esplora la guida

- Le migliori pratiche per AWS Secrets Manager

  Scopri le migliori pratiche da prendere in considerazione durante l'utilizzo AWS Secrets Manager.

  Esplora la guida

- AWS Secrets Manager prezzi

  Consulta la pagina AWS Secrets Manager dei prezzi per scoprire i costi associati all'archiviazione, alla gestione e al recupero in modo sicuro di segreti come le credenziali del database e le chiavi API.

Esplora la pagina dei prezzi

- AWS Secrets Manager Domande frequenti

  AWS Secrets Manager Consulta la pagina delle domande frequenti per risposte dettagliate alle domande più comuni AWS Secrets Manager, comprese le funzionalità, le misure di sicurezza, i prezzi e le capacità di integrazione.

  Esplora il FAQs

Esplora

- Ricerca e risorse

  Esplora AWS blog, video e strumenti sulla crittografia.

  Rivedi le risorse
- Video

  Guardate questi video dal canale AWS Developers per sviluppare e YouTube perfezionare ulteriormente la vostra strategia di crittografia.

  Esplora i video sulla crittografia

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti a questa guida decisionale. Per ricevere notifiche sugli aggiornamenti di questa guida, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	Guida pubblicata per la prima volta.	31 gennaio 2025

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.