Service Name

AWS CloudHSM

Service Overview

AWS CloudHSM is a cloud-based hardware security module (HSM) service that enables customers to generate and manage their own encryption keys using dedicated, FIPS 140-2 Level 3 validated HSMs. The service provides complete control over high-availability HSMs in the AWS Cloud with low-latency access and secure cryptographic operations. CloudHSM combines the benefits of AWS cloud scalability with the security of hardware security modules, offering single-tenant access to computing devices that process cryptographic operations and provide secure storage for cryptographic keys. The service automates HSM management including backups, provisioning, configuration, and maintenance while ensuring customers retain full control over their encryption keys and cryptographic operations.

Key Use Cases

- Regulatory compliance: Meet corporate, contractual, and regulatory compliance requirements for data security using dedicated HSMs that comply with PCI DSS, PCI PIN, and PCI-3DS standards
- Database encryption: Enable Transparent Data Encryption (TDE) for databases by storing TDE master encryption keys in HSMs to encrypt database files with enhanced security
- SSL/TLS processing offload: Offload SSL/TLS processing for web servers to reduce computational burden and provide additional security for high-traffic applications
- Certificate Authority (CA) operations: Store and manage private keys for certificate authorities to maintain trust and perform cryptographic signing operations for PKI infrastructure
- Document signing and verification: Create asymmetric public and private key pairs for digitally signing and verifying documents to ensure authenticity and integrity
- Message authentication: Securely create and manage symmetric keys for CMACs and HMACs to authenticate messages and ensure message integrity
- Code and firmware signing: Sign applications and firmware using private keys stored in HSMs to establish trust and prevent unauthorized code execution
- Key management integration: Combine with AWS KMS to store key material in a single-tenant environment while leveraging AWS KMS benefits for integrated AWS services
- Random number generation: Securely generate cryptographically strong random numbers in HSMs for creating encryption keys and other security tokens

Features

- **FIPS Validated HSMs**: FIPS 140-2 Level 3 and FIPS 140-3 Level 3 validated hardware security modules for clusters in FIPS mode, with non-FIPS mode available for broader algorithm support
- **Industry-Standard APIs**: Support for PKCS#11, Java Cryptography Extensions (JCE), Microsoft CryptoNG (CNG), and Key Storage Provider (KSP) APIs for seamless application integration
- **High Availability Clustering**: Multi-AZ cluster deployment with automatic synchronization and load balancing across multiple HSMs for 99.95% uptime SLA
- **Automatic Backup Management**: Automated daily backups with configurable retention policies, cross-region backup copying, and cluster restore capabilities
- **Single-Tenant Architecture**: Dedicated HSM instances with complete isolation from other customers and full customer control over keys and cryptographic operations
- **Scalable Performance**: Up to 10,000 cryptographic operations per second with support for up to 28 HSMs per cluster and storage for up to 16,666 keys
- **Client SDK Integration**: Comprehensive client SDKs for multiple platforms including Linux and Windows with CloudHSM CLI for cluster management
- **Third-Party Integrations**: Native support for Oracle TDE, SSL offload, Windows CA, and integration with third-party vendors like HashiCorp Vault and PrimeKey EJBCA

Value Proposition

AWS CloudHSM provides customers with dedicated, single-tenant hardware security modules that offer complete control over cryptographic operations while leveraging AWS cloud benefits. Unlike managed services, CloudHSM gives customers full ownership of encryption keys with end-to-end encryption invisible to AWS:

- The service offers superior security through FIPS 140-2/140-3 Level 3 validation, ensuring compliance with stringent regulatory requirements
- Key advantages include seamless migration support for existing PKCS#11, JCE, and CNG applications, automatic high availability across multiple AZs, and integration with industry-standard cryptographic APIs
- The fully managed infrastructure eliminates hardware procurement, maintenance, and patching overhead while providing elastic scalability and global availability across multiple AWS regions

Service Integration

AWS CloudHSM integrates with Amazon VPC for network isolation and secure connectivity to EC2 instances running client applications. Integration with AWS KMS enables custom key stores, allowing customers to combine CloudHSM's single-tenant security with KMS's seamless AWS service integration for services like S3, EBS, and RDS:

- CloudWatch provides monitoring and alerting for HSM health and performance metrics
- CloudTrail logs all AWS CloudHSM API calls for audit and compliance purposes
- The service works with AWS Direct Connect and VPN for hybrid connectivity, enabling secure communication between on-premises applications and cloud-hosted HSMs
- Integration with IAM provides access control for CloudHSM management operations, while AWS Backup can be used for additional backup orchestration across AWS services

Onboarding and Offboarding

Getting started with AWS CloudHSM involves creating a VPC and subnets across multiple availability zones, then creating a CloudHSM cluster through the console, CLI, or API. Customers must initialize the cluster with a self-signed certificate, add HSMs to achieve desired availability and performance, and install the CloudHSM client software on EC2 instances:

- The process includes configuring security groups for HSM communication, activating the cluster using CloudHSM CLI, creating HSM users (crypto officers and crypto users), and integrating applications using supported APIs like PKCS#11 or JCE
- AWS provides comprehensive documentation, sample code, and getting started guides
- Setup typically requires network configuration knowledge and understanding of cryptographic concepts, but AWS offers professional services support for complex implementations

Getting Started Guide: https://docs.aws.amazon.com/cloudhsm/latest/userguide/getting-started.html

Data Removal

To offboard from AWS CloudHSM, customers must export any required keys using supported APIs before deleting HSMs and clusters. The process involves stopping client applications, removing HSMs from clusters using the console or CLI, and deleting the cluster itself. All HSMs must be removed before cluster deletion. Customer data in HSMs is automatically destroyed when HSMs are deleted due to tamper-resistant hardware design. Backup data can be explicitly deleted through on-demand backup deletion features, though backups are retained for 7 days after deletion requests for recovery purposes.

Backup/Restore and Disaster Recovery

AWS CloudHSM automatically creates encrypted backups of clusters at least once every 24 hours, including all user data, key material, certificates, and HSM configuration. Backups can be copied across AWS regions for disaster recovery and used to create new clusters in different regions. The service supports configurable backup retention policies with automatic purging of expired backups. Customers can restore entire clusters from backups and force backup creation by adding/removing HSMs. Multi-AZ cluster deployment provides high availability with automatic failover between HSMs in different availability zones.

Backup Capabilities

AWS CloudHSM includes native automated backup capabilities with daily encrypted backups stored securely by AWS. The service provides managed backup retention policies, on-demand backup deletion through AWS SDK and CLI, and cross-region backup copying for geographic distribution:

- While AWS CloudHSM does not directly integrate with AWS Backup service, its comprehensive built-in backup features provide robust data protection
- Backups include complete cluster state including keys, users, and configurations, enabling full cluster restoration

Disaster Recovery

AWS CloudHSM supports disaster recovery through multi-AZ cluster deployment, cross-region backup copying, and the ability to create clusters from backups in different regions. The service does not directly integrate with AWS Elastic Disaster Recovery, but provides comprehensive DR capabilities through its native backup and clustering features. Customers can implement cross-region disaster recovery by copying backups to secondary regions and creating standby clusters when needed.

Recovery Objectives

AWS CloudHSM supports low RTO objectives through multi-AZ high availability clustering with automatic failover between HSMs in different availability zones. RPO objectives are met through automated daily backups with the ability to force more frequent backups as needed. Cross-region backup copying enables geographic disaster recovery. The 99.95% uptime SLA for multi-AZ clusters helps meet stringent availability requirements. Customers can achieve near-zero RTO within a region through cluster redundancy and low RPO through frequent backup operations.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/cloudhsm/latest/userguide/limits.html

FAQ: https://aws.amazon.com/cloudhsm/faqs/

Technical Requirements

Service Documentation:
https://docs.aws.amazon.com/cloudhsm/latest/userguide/introduction.html

User Guide: https://docs.aws.amazon.com/cloudhsm/latest/userguide/introduction.html

API Reference:
https://docs.aws.amazon.com/cloudhsm/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/cloudhsm/pricing/

Cost Optimization

AWS CloudHSM offers unique cost optimization through pay-as-you-go hourly pricing with no upfront costs or long-term commitments. Customers can dynamically scale HSM capacity by adding or removing HSMs based on workload demands:

- The service eliminates capital expenses for HSM hardware, maintenance, and facilities
- Costs are optimized through managed backup retention policies that automatically purge expired backups, and on-demand backup deletion capabilities
- Regional deployment flexibility allows customers to choose cost-effective regions while maintaining compliance requirements
- The fully managed service reduces operational overhead and staffing costs compared to on-premises HSM management

Savings Considerations

Primary cost savings include elimination of hardware procurement, maintenance, and replacement costs for physical HSMs. Customers avoid facility requirements including secure data centers, power, cooling, and physical security infrastructure:

- The managed service reduces operational staffing needs for HSM maintenance, firmware updates, and hardware monitoring
- Elastic scaling prevents over-provisioning by allowing HSM capacity adjustment based on actual demand
- Automated backup management reduces storage costs through intelligent retention policies
- No reserved instance pricing is offered, but the pay-per-hour model provides cost predictability

- Cross-region backup copying eliminates need for separate disaster recovery infrastructure investments