AWS CloudHSM

## **I. What is AWS CloudHSM?**

[AWS CloudHSM](https://aws.amazon.com/cloudhsm/) is a cloud-based hardware security module that provides secure cryptographic key storage and operations within a tamper-resistant hardware device. This service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using FIPS 140-2 Level 3 validated HSMs.

## **II. AWS CloudHSM Features and Advantages**

### **A. Secure Key Storage**

AWS CloudHSM allows you to generate, store, and manage cryptographic keys securely.

### **B. FIPS 140-2 Level 3 Compliance**

The service meets [high compliance standards](https://en.wikipedia.org/wiki/FIPS_140-2), ensuring your data’s security.

### **C. Scalability**

AWS CloudHSM is fully scalable, allowing you to increase capacity as needed.

### **D. Flexibility**

It supports multiple APIs, including [PKCS#11](https://www.ibm.com/docs/en/linux-on-systems?topic=introduction-what-is-pkcs-11), [Java Cryptography Extensions (JCE)](https://www.oracle.com/java/technologies/javase-jce-all-downloads.html), and [Microsoft CryptoNG (CNG)](https://learn.microsoft.com/en-us/windows/win32/seccng/cng-portal) libraries.

### **E. Control and Independence**

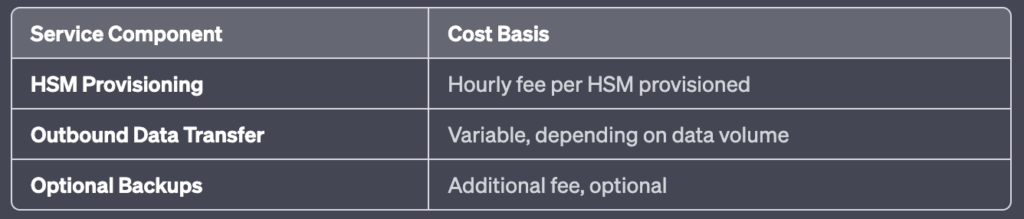
Users have exclusive, single-tenant access to each HSM in their cluster.

## **III. AWS CloudHSM Monitoring**

AWS CloudHSM integrates with [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) and [Amazon CloudWatch](https://aws.amazon.com/cloudwatch/). CloudTrail records API calls for your account, while CloudWatch allows you to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

## 

## **IV. AWS CloudHSM Pricing**

****

Please note, the actual costs can vary based on different regions and specific usage patterns. Always refer to the official [AWS Pricing page](https://aws.amazon.com/pricing/?nc2=h_ql_pr_ln&aws-products-pricing.sort-by=item.additionalFields.productNameLowercase&aws-products-pricing.sort-order=asc&awsf.Free%20Tier%20Type=*all&awsf.tech-category=*all) for the most accurate and up-to-date information.

## **V. AWS CloudHSM Use Cases**

### **A. Protect Private Keys for an Issuing CA**

AWS CloudHSM can securely generate and store the private key of a root or intermediate CA, reducing the risk of unauthorized access.

### **B. Offload SSL Processing for Web Servers**

The service can offload SSL/TLS processing from web servers, improving website performance.

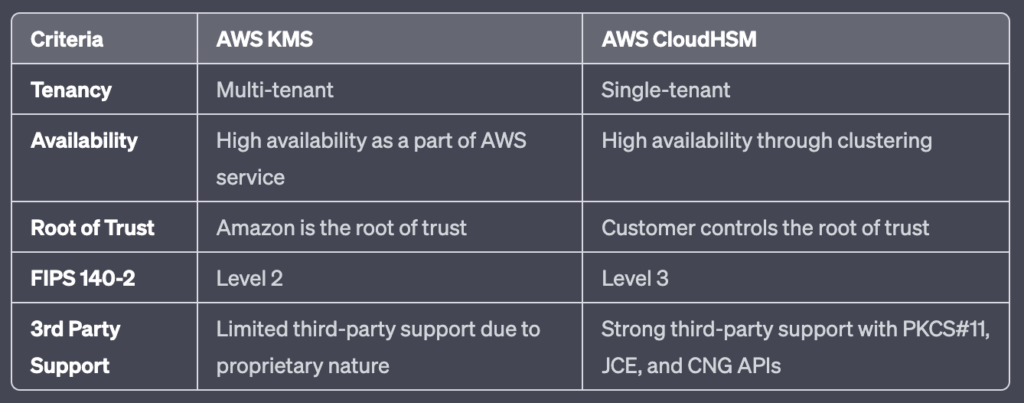
### **C. Encrypt Data at Rest**

AWS CloudHSM enables the encryption of data at rest, providing an additional layer of protection for sensitive data.

## 

## **VI. AWS CloudHSM FAQs**

### **A. What is the difference between AWS KMS and AWS CloudHSM?**

****

### **B. When should I use AWS CloudHSM instead of AWS KMS?**

AWS CloudHSM is recommended when you need to control and manage your own encryption keys in single-tenant hardware, or when you have compliance requirements that cannot be met by AWS KMS.

### **C. What level of compliance is CloudHSM?**

AWS CloudHSM is compliant with FIPS 140-2 Level 3, one of the highest levels of compliance for data security. This signifies that it meets stringent requirements for physical tamper-resistance, role-based access control, and ability to zeroize all plaintext cryptographic keys and critical security parameters within the module. This level of certification provides assurance that CloudHSM is designed to prevent unauthorized physical and logical access to cryptographic keys, making it suitable for handling sensitive data.

## **VII. Conclusion**

AWS CloudHSM offers a robust platform that enables organizations to generate, store, and manage encryption keys securely in the cloud. The service’s flexibility comes from its support for various APIs and its scalability from the ability to increase capacity on-demand. With its high compliance standards, including FIPS 140-2 Level 3, it ensures stringent security for cryptographic operations. As such, businesses seeking a solution for securely managing cryptographic keys, while maintaining control and meeting compliance requirements, will find AWS CloudHSM to be a highly suitable service.

*Note: Last updated May 15, 2023*

### 

### **Related posts:**

* ****