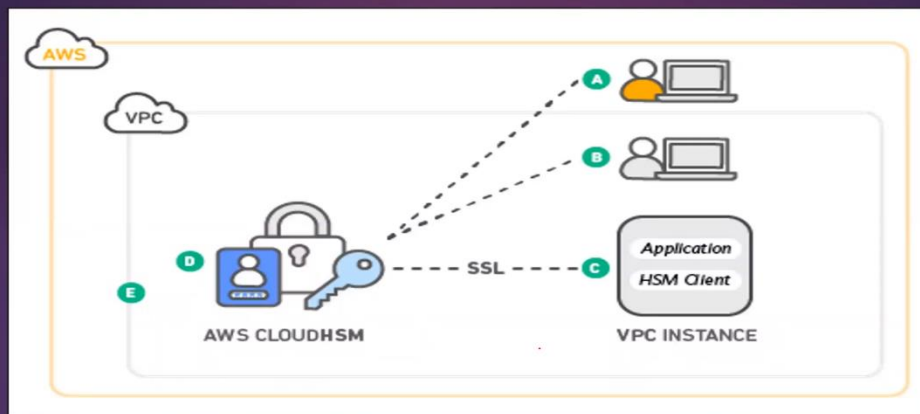


## CloudHSM

### What is Cloud Hardware Security Module (HSM)?

- A **hardware security module (HSM)** is a computing device that processes cryptographic operations and provides secure storage for cryptographic keys
- AWS **CloudHSM** is a **cloud-based** hardware security module (HSM) that enables you to generate and use your own encryption keys
- CloudHSM is a **compliant** with **FIPS 140-2 Level 3** (The **Federal Information Processing Standard** Publication 140-2)
- It **automates administrative tasks** like hardware provisioning, software patching, high-availability, and backups
- **Applications** can **integrate** with CloudHSM using **PKCS#11**, **Java Cryptography Extensions (JCE)**, and **Microsoft CryptoNG (CNG) API** libraries
- CloudHSM can **scale quickly** on-demand with no up-front costs

### How does CloudHSM work?




- AWS **CloudHSM** provides hardware security modules (HSMs) in a **cluster**
- A **cluster** is one **logical** HSM
- To interact with the HSMs in a cluster, you need the AWS CloudHSM client software.
- Client can be installed on Amazon EC2 instances, known as client instances, that reside in the same VPC as the HSM ENIs,
- When you perform a task or **operation on one HSM** in a cluster, the **other HSMs** in that cluster are **automatically updated**.
- You can create a **cluster** that has from **1 to 28 HSMs** (the default limit is 6 HSMs per AWS account per AWS Region)

## [AMAZONE WEB SERVICES –30-CloudHSM]

**AWS CloudHSM** [Overview](#) [Features](#) [Pricing](#) [Getting Started](#) [Resources](#) [FAQs](#)


### Offload the SSL processing for web servers

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are used to confirm the identity of web servers and establish secure HTTPS connections over the Internet. You can use AWS CloudHSM to offload SSL/TLS processing for your web servers. Using CloudHSM for this processing reduces the burden on your web server and provides extra security by storing your web server's private key in CloudHSM.




### Protect private keys for an issuing certificate authority (CA)

In a public key infrastructure (PKI), a certificate authority (CA) is a trusted entity that issues digital certificates. These digital certificates are used to identify a person or organization. You can use AWS CloudHSM to store your private keys and sign certificate requests so that you can securely act as an issuing CA to issue certificates for your organization.



### Enable Transparent Data Encryption (TDE) for Oracle databases

You can use AWS CloudHSM to store the Transparent Data Encryption (TDE) master encryption key for your Oracle database servers that support TDE. Support for SQL Server is coming soon. With TDE, supported database servers can encrypt data before storing it on disk. Please note Amazon RDS for Oracle does not support TDE with CloudHSM; you should use AWS Key Management Service for this use case.



## Benefits

- **Generate and manage** cryptographic keys
- **Cluster based** makes it easy to **load balance** and **scale**
- **API based integration** for **Applications**
- **Integrates** with **AWS KMS** to create **custom key stores**

## Price

- Pay by the hour with no long-term commitments or upfront payments.