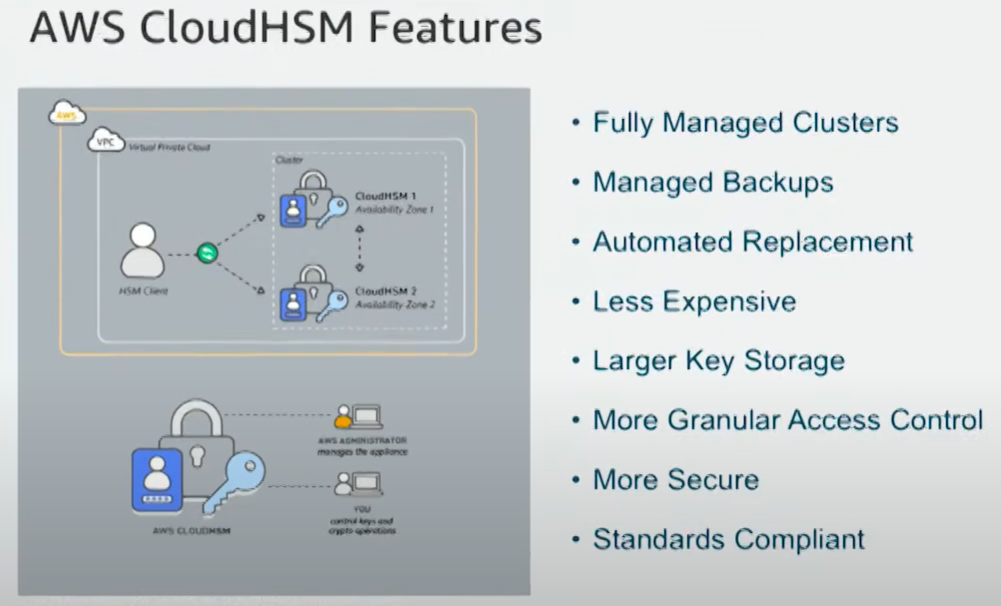
AWS CloudHSM

# AWS CloudHSM

* AWS CloudHSM provides secure cryptographic key storage to customers by making hardware security modules (HSMs) available in the AWS cloud
* AWS CloudHSM helps meet corporate, contractual and regulatory compliance requirements for data security by using dedicated HSM appliances within the AWS cloud.
* A hardware security module (HSM)
  + is a hardware appliance that provides secure key storage and cryptographic operations within a tamper-resistant hardware module.
  + are designed with physical and logical mechanisms, to securely store cryptographic key material and use the key material without exposing it outside the cryptographic boundary of the appliance.
  + physical protections include tamper detection and tamper response. When a tampering event is detected, the HSM is designed to securely destroy the keys rather than risk compromise
  + logical protections include role-based access controls that provide separation of duties
* CloudHSM allows encryption keys protection within HSMs, designed and validated to government standards for secure key management.
* CloudHSM helps comply with strict key management requirements within the AWS cloud without sacrificing application performance
* **CloudHSM uses SafeNet Luna SA HSM appliances**
* HSMs are located in AWS data centers, managed and monitored by AWS, but AWS does not have access to the keys
* AWS can’t help recover the key material if the credentials are lost
* HSMs are inside your VPC and isolated from the rest of the network
* CloudHSM provides single tenant dedicated access to each HSM appliance
* Placing HSM appliances near your EC2 instances decreases network latency, which can improve application performance
* Only you have access to the keys and operations to generate, store and manage on the keys
* Integrated with Amazon Redshift and Amazon RDS for Oracle
* Other use cases like EBS volume encryption and S3 object encryption and key management can be handled by writing custom applications and integrating them with CloudHSM



Usecases :

* Offload SSL processing for webserver.
* Protect private keys for an issuing certificate authority.
* Enable Transparent Data Encryption (TDE) for Oracle databases

## AWS Certification Exam Practice Questions

1. With which AWS services CloudHSM can be used (select 2)
   1. S3
   2. DynamoDb
   3. **RDS**
   4. ElastiCache
   5. **Amazon Redshift**
2. An AWS customer is deploying a web application that is composed of a front-end running on Amazon EC2 and of confidential data that is stored on Amazon S3. The customer security policy that all access operations to this sensitive data must be authenticated and authorized by a centralized access management system that is operated by a separate security team. In addition, the web application team that owns and administers the EC2 web front-end instances is prohibited from having any ability to access the data that circumvents this centralized access management system. Which of the following configurations will support these requirements:
   1. Encrypt the data on Amazon S3 using a CloudHSM that is operated by the separate security team. Configure the web application to integrate with the CloudHSM for decrypting approved data access operations for trusted end-users. (S3 doesn’t integrate directly with CloudHSM, also there is no centralized access management system control)
   2. **Configure the web application to authenticate end-users against the centralized access management system. Have the web application provision trusted users STS tokens entitling the download of approved data directly from Amazon S3**(Controlled access and admins cannot access the data as it needs authentication)
   3. Have the separate security team create and IAM role that is entitled to access the data on Amazon S3. Have the web application team provision their instances with this role while denying their IAM users access to the data on Amazon S3 (Web team would have access to the data)
   4. Configure the web application to authenticate end-users against the centralized access management system using SAML. Have the end-users authenticate to IAM using their SAML token and download the approved data directly from S3. (not the way SAML auth works and not sure if the centralized access management system is SAML complaint)