Security of AWS CloudHSM Backups

Fully Managed Hardware Security Modules (HSMs) in the AWS Cloud

December 2017

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

AWS CloudHSM clusters provide high availability and redundancy by distributing cryptographic operations across all hardware security modules (HSMs) in the cluster. Backup and restore is the mechanism by which a new HSM in a cluster is synchronized. This whitepaper provides details on the cryptographic mechanisms supporting backup and restore functionality, and the security mechanisms protecting the AWS-managed backups. This whitepaper also provides in-depth information on how backups are protected in all three phases of the CloudHSM backup lifecycle process: Creation, Archive, and Restore.

For the purposes of this whitepaper, we assume that you have a basic understanding of AWS CloudHSM and cluster architecture.

Introduction

Amazon Web Services (AWS) offers two options for securing cryptographic keys in the AWS Cloud: AWS Key Management Service (AWS KMS) and AWS CloudHSM. AWS KMS is a managed service that uses hardware security modules (HSMs) to protect the security of your encryption keys. AWS CloudHSM delivers fully managed HSMs in the AWS Cloud, which allows you to add secure, validated key storage and high-performance crypto acceleration to your AWS applications. CloudHSM offers you the option of single-tenant access and control over your HSMs. CloudHSM is based on FIPS 140-2 Level 3 validated hardware.

CloudHSM delivers fully managed HSMs in the AWS Cloud. CloudHSM delivers all the benefits of traditional HSMs including secure generation, storage, and management of cryptographic keys used for data encryption that are controlled and accessible only by you. As a managed service, it also automates time-consuming administrative tasks such as hardware provisioning, software patching, high availability, and backups.

HSM capacity can be scaled quickly by adding and removing HSMs from your cluster on demand. The backup and restore functionality of CloudHSM is what enables scalability, reliability, and high availability in CloudHSM. A key aspect of the backup and restore feature is a secure backup protocol that CloudHSM uses to back up your cluster. This paper takes an in-depth look at the security mechanisms in place around this feature.

AWS CloudHSM: Managed by AWS, Controlled by You

AWS CloudHSM provides HSMs in a cluster. A cluster is a collection of individual HSMs that AWS CloudHSM keeps in sync. You can think of a cluster as one logical HSM. When you perform a key generation task or operation on one HSM in a cluster, the other HSMs in that cluster are automatically kept up to date. Each HSM in a cluster is a single-tenant HSM under your control. At the hardware level, each HSM includes hardware-enforced isolation of crypto operations and key storage. Each HSM runs on dedicated cryptographic cores.

Each HSM appears as a network resource in your virtual private cloud (VPC). AWS manages the HSM on your behalf, performing functions such as health checks, backups, and synchronization of HSMs within a cluster. However, you alone control the user accounts, passwords, login policies, key rotation procedures, and all aspects of configuring and using the HSMs. The implication of this control is that your cryptographic data is secure from external compromise. This is important to financial applications subject to PCI regulations, healthcare applications subject to HIPAA regulations, and streaming video solutions subject to contractual DRM requirements.

You interact with the HSMs in a cluster via the AWS CloudHSM client. Communication occurs over an end-to-end encrypted channel. AWS does not have visibility into your communication with your HSM, which occurs within this end-to-end encrypted channel.

High Availability

Historically, deploying and maintaining traditional HSMs in a high-availability configuration has been a manual process that is cumbersome and expensive. CloudHSM makes scalability and high availability simple without compromising security.

When you use CloudHSM you begin by creating a cluster in a particular AWS Region. A cluster can contain multiple individual HSMs. For idle workloads, you can delete all HSMs and simply retain the empty cluster. For production workloads, you should have at least two HSMs spread across multiple Availability Zones. CloudHSM automatically synchronizes and load balances the HSMs within a cluster.

The CloudHSM client load-balances cryptographic operations across all HSMs in the cluster based on the capacity of each HSM for additional processing. If a cluster requires additional throughput, you can expand your cluster by adding more HSMs through a single API call or a click in the CloudHSM console.

When you expand a cluster, CloudHSM automatically provisions a new HSM as a clone of the other HSMs in the cluster. This is done by taking a backup of an existing HSM and restoring it to the newly added HSM. When you delete an HSM from a cluster, a backup is automatically taken. This way, when you create a new HSM later, you can pick up where you left off. Should an HSM fail for any

reason, the service will automatically replace it with a new, healthy HSM. This HSM is restored from a backup of another HSMs in the cluster if available. Otherwise, the new HSM is restored from the last available backup taken for the cluster.

When you don't need to use a cluster any more, you can delete all its HSMs, as well as the cluster. Later, when you need to use the HSMs again, you can create a new cluster from the backup, effectively restoring your previous HSM.

In the next section, we will take a deeper look at the contents of the backup and the security mechanisms used to protect it.

CloudHSM Cluster Backups

Backups are initiated, archived, and restored by CloudHSM. A *backup* is a complete, encrypted snapshot of the HSM. Each AWS-managed backup contains the entire contents of the HSM, including keys, certificates, users, policies, quorum settings, and configuration options. This includes:

- Certificates on the HSM, including the cluster certificate[1]
- All HSM users (COs, CUs, and AU)[2]
- All key material on the HSM
- HSM configurations and policies

Backups are stored in Amazon Simple Storage Service (Amazon S3) within the same Region as the cluster. You can view backups available for your cluster from the CloudHSM console. Backups can only be restored to a genuine HSM running in the AWS Cloud. The restored HSM retains all the configurations and policies you put in place on the original HSM.

Creating a Backup

CloudHSM triggers backups in the following scenarios:

- CloudHSM automatically backs up your HSM clusters periodically.
- When adding an HSM to a cluster, CloudHSM takes a backup from an active HSM in that cluster and restores it to the newly provisioned HSM.

- When deleting an HSM from a cluster, CloudHSM takes a backup of the HSM before deleting it.

A backup is a unified encrypted object combining certificates, users, keys, and policies. It is created and encrypted as a single, tightly-bound object. The individual components are not separable from each other. The key used to encrypt the backup is derived using a combination of persistent and ephemeral secret keys. Backups are encrypted and decrypted within your HSM only, and can only be restored to a genuine HSM running within the AWS Cloud. This is discussed in further detail in the section Security of Backups: Restoration of Backups. CloudHSM uses FIPS 140-2 level 3 validated HSMs. Your cryptographic material is never accessible in the clear outside the hardware.

Archiving a Backup

CloudHSM stores the cluster backups in a service-controlled Amazon S3 location in the same AWS Region as your cluster. The following figure illustrates an encrypted backup of an HSM cluster in a service-controlled Amazon S3 bucket.

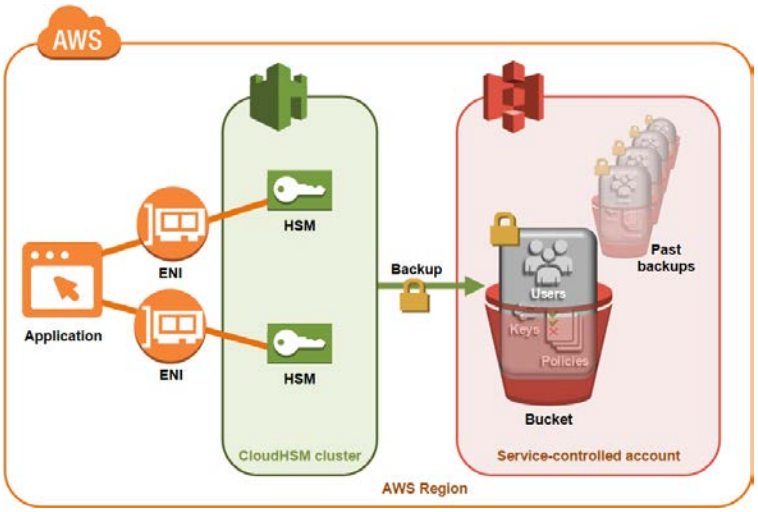

Figure 1: Encrypted backup of an HSM cluster in a service-controlled S3 bucket

Restoring a Backup

Backups are used in two scenarios:

- When you provision a new cluster using an existing backup

- When a second (or subsequent) HSM is added to a cluster, or when CloudHSM automatically replaces an unhealthy HSM

In both scenarios, the backup is restored to a newly created HSM. During restoration, the backup is decrypted within an HSM, using the process described in the next section. The decryption relies on a set of keys available only within an authentic hardware instance from the original manufacturer, installed in the AWS Cloud. Therefore, CloudHSM can restore backups onto only authentic HSMs within the AWS Cloud.

Recall that each backup contains all users, keys, access policies, and configuration from the original HSM. Therefore, the restored HSM contains the same protections and access controls as the original and is equivalently secure to the original. When your application or cryptographic officer seeks to use the HSM, you can verify that the HSM is a clone of the one you originally established a trust relationship with. You do so by confirming that the cluster certificate is signed using the same key you used when initially claiming the HSM. This ensures that you are talking to your HSM.

Note that while CloudHSM manages backups, the service does not have any access to the data, cryptographic material, user information, and the keys encapsulated within the backup. Specifically, AWS has no way to recover your keys if you lose your access credentials to log in to the HSM.

Security of Backups

The CloudHSM backup mechanism has been validated under FIPS 140-2 Level 3.[3] A backup taken by an HSM configured in FIPS-mode cannot be restored to an HSM that is not also in FIPS-mode. Operation in FIPS-mode is a required configuration for CloudHSM. An HSM in FIPS-mode is running production firmware provided by the manufacturer and signed with a FIPS production key. This ensures other parties cannot forge the firmware. Furthermore, each backup contains a complete copy of everything in the HSM. Specifically, each AWS-managed backup contains the entire contents of the HSM, including keys, claiming certificates, users, policies, quorum settings, and configuration options. Accordingly, you can demonstrate – for example, during a compliance audit - that each HSM with a restored backup is protected at exactly the same level and with the same policies and controls as when the backup was first created.

Key Hierarchy

As discussed earlier, a backup is encrypted within the HSM before it is provided to CloudHSM for archival. The backup is encrypted using a backup encryption key, described in the following section.

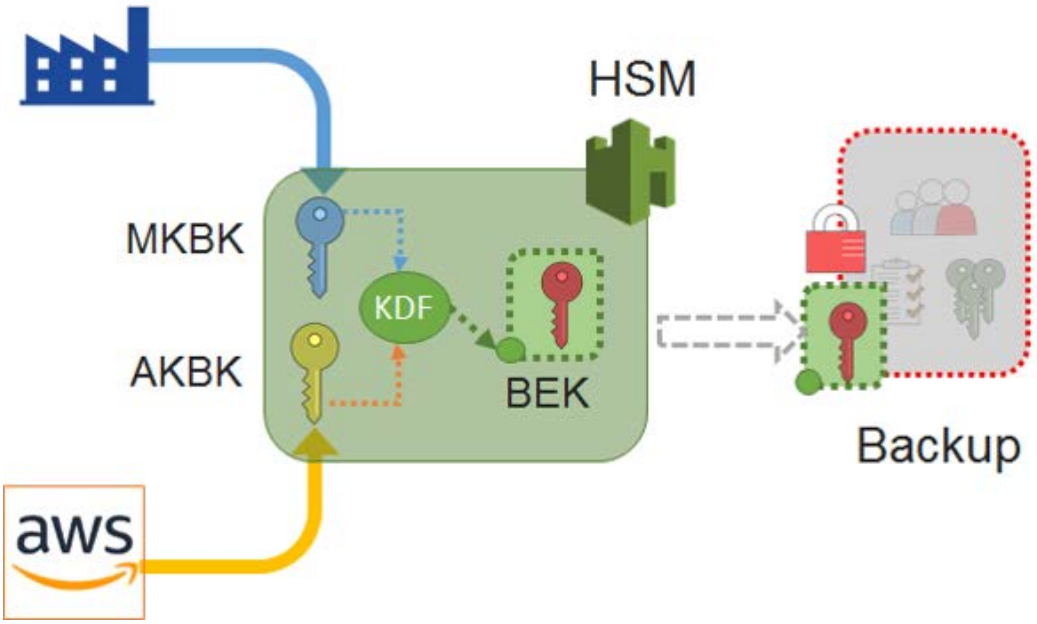

Figure 2: The backup of the HSM is encrypted using a backup encryption key (BEK)

Manufacturer's Key Backup Key (MKBK)

The manufacturer's key backup key (MKBK) exists in the HSM hardware provided by the manufacturer. This key is common to all HSMs provided by the manufacturer to AWS. The MKBK cannot be accessed or used by any user or for any purpose other than the generation of the backup encryption key. Specifically, AWS does not have access to or visibility into the MKBK.

AWS Key Backup Key (AKBK)

The AWS key backup key (AKBK) is securely installed by the CloudHSM service when the hardware is placed into operation within the CloudHSM fleet. This key is unique to hardware installed by AWS within our CloudHSM infrastructure. The AKBK is generated securely within an offline FIPS-compliant hardware security module, and loaded under two-person control into newly commissioned CloudHSM hardware.

Backup Encryption Key (BEK)

The backup of the HSM is encrypted using a backup encryption key (BEK). The BEK is an AES-256 key that is generated within the HSM when a backup is requested. The HSM uses the BEK to encrypt its backup. The encrypted backup includes a wrapped copy of the BEK.

The BEK is wrapped with an AES 256-bit wrapping key using a FIPS-approved AES key wrapping method. This method complies with NIST Special Publication 800-38F. The wrapping key is derived from the MKBK and AKBK via a key derivation function (KDF). This same wrapping key must be derived again to recover the BEK prior to decrypting the backup. This implies that both the MKBK and AKBK are required to decrypt a customer backup. Put another way, the BEK cannot be discovered or derived using a secret managed by AWS or by the manufacturer alone. Once encrypted, the backup is ready to be archived. Recall that each backup is stored on Amazon S3.

Restoration of Backups

CloudHSM backups can only be decrypted by an HSM that is able to derive the same wrapping key used to secure the BEK when the backup was created. Recall that this wrapping key is derived from the Manufacturer's Key Backup Key (MKBK) and the AWS Key Backup Key (AKBK). The MKBK is only embedded in genuine hardware by the manufacturer, and the AKBK is only installed on genuine hardware within the AWS fleet. Therefore, the BEK cannot be unwrapped outside of an AWS-managed HSM. This in turn implies that the backup cannot be decrypted outside of an AWS-managed HSM.

Conclusion

AWS CloudHSM provides a secure, FIPS-validated HSM backup and restore mechanism that enables high-availability and failure management capabilities without sacrificing security or privacy. You retain complete control over your HSM and the data within. Backups are encrypted strongly at creation, stored securely, and never decrypted outside an HSM. Backups can only be restored to genuine hardware in the AWS Cloud, running firmware signed with a FIPS production key. As backups include user accounts and security policy configurations in addition to cryptographic material, restored HSMs retain all the security policies and controls from the original HSM. With CloudHSM, you can demonstrate – for example during a compliance audit – that an HSM

restored from backup is protected at exactly the same level and with the same policies and controls as the HSM from which the backup was originally created.

Contributors

The following individuals and organizations contributed to this document:

- Ben Grubin, General Manager, AWS Cryptography
- Balaji Iyer, Senior Professional Services Consultant, AWS
- Avni Rambhia, Senior Product Manager, AWS Cryptography

Further Reading

- CloudHSM guide: https://aws.amazon.com/documentation/cloudhsm/
- CloudHSM product details: https://aws.amazon.com/cloudhsm/details/
- Blog - Cost Effective Hardware Key Management at Cloud Scale for Sensitive & Regulated Workloads: https://aws.amazon.com/blogs/aws/aws-cloudhsm-update-cost-effective-hardware-key-management/
- Webinar - Secure Scalable Key Storage in AWS: https://www.youtube.com/watch?v=hEVks207ALM
- Verify the Identity and Authenticity of Your Cluster's HSM: http://docs.aws.amazon.com/cloudhsm/latest/userguide/verify-hsm-identity.html
- AWS CloudHSM Client Tools and Software Libraries: http://docs.aws.amazon.com/cloudhsm/latest/userguide/client-tools-and-libraries.html#client

Notes

[1] http://docs.aws.amazon.com/cloudhsm/latest/userguide/initialize-cluster.html

[2] http://docs.aws.amazon.com/cloudhsm/latest/userguide/hsm-users.html

[3] https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2850.pdf