AWS CloudHSM FAQs

Q: What is AWS CloudHSM?

The AWS CloudHSM service helps you meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are designed and validated to government standards for secure key management. CloudHSM allows you to securely generate, store, and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Q: What is a Hardware Security Module (HSM)?

A Hardware Security Module (HSM) provides secure key storage and cryptographic operations within a tamper-resistant hardware device. HSMs are designed to securely store cryptographic key material and use the key material without exposing it outside the cryptographic boundary of the hardware.

Q: What can I do with CloudHSM?

You can use the CloudHSM service to support a variety of use cases and applications, such as database encryption, Digital Rights Management (DRM), Public Key Infrastructure (PKI), authentication and authorization, document signing, and transaction processing.

Q: How does CloudHSM work?

When you use the AWS CloudHSM service you create a CloudHSM Cluster. Clusters can contain multiple HSM instances, spread across multiple Availability Zones in a region. HSM instances in a cluster are automatically synchronized and load-balanced. You receive dedicated, single-tenant access to each HSM instance in your cluster. Each HSM instance appears as a network resource in your Amazon Virtual Private Cloud (VPC). Adding and removing HSMs from your Cluster is a single call to the AWS CloudHSM API (or on the command line using the AWS CLI). After creating and initializing a CloudHSM Cluster, you can configure a client on your EC2 instance that allows your applications to use the cluster over a secure, authenticated network connection.

Amazon administrators monitor the health of your HSMs, but do not have any access to configure, manage, or use them. Your applications use standard cryptographic APIs, in conjunction with HSM client software installed on the application instance, to send cryptographic requests to the HSM. The client software maintains a secure channel to all of the HSMs in your cluster and sends requests on this channel, and the HSM performs the operations and returns the results over the secure channel. The client then returns the result to the application through the cryptographic API.

Q: I don’t currently have a VPC. Can I still use AWS CloudHSM?

No. To protect and isolate your AWS CloudHSM from other Amazon customers, CloudHSM must be provisioned inside an Amazon VPC. Creating a VPC is easy. Please see the [VPC Getting Started Guide](http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/ExerciseOverview.html) for more information.

Q: Does my application need to reside in the same VPC as the CloudHSM Cluster?

No, but the server or instance on which your application and the HSM client are running must have network (IP) reachability to all HSMs in the cluster. You can establish network connectivity from your application to the HSM in many ways, including operating your application in the same VPC, with VPC peering, with a VPN connection, or with Direct Connect. Please see the [VPC Peering Guide](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html) and [VPC User Guide](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide) for more details.

Q: Does CloudHSM work with on-premises HSMs?

Yes. While CloudHSM does not interoperate directly with on-premises HSMs, you can securely transfer exportable keys between CloudHSM and most commercial HSMs using one of several supported RSA key wrap methods.

Q: How can my application use CloudHSM?

We have integrated and tested CloudHSM with a number of third-party software solutions such as Oracle Database 11g and 12c and Web servers including Apache and Nginx for SSL offload. Please see the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for more information.

If you are developing your own custom application, your application can use the standard APIs supported by CloudHSM, including PKCS#11 and Java JCA/JCE (Java Cryptography Architecture/Java Cryptography Extensions). Support for Microsoft CAPI/CNG is coming soon. Please refer to the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for code samples and help with getting started.

If you are moving an existing workload from CloudHSM Classic or on-premises HSMs to CloudHSM, our [CloudHSM migration guide](https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Docs/CloudHSMUpgradeGuide-latest.pdf) provides information on how to plan and execute your migration.

Q: Can I use CloudHSM to store keys or encrypt data used by other AWS services?

Yes. You can do all encryption in your CloudHSM-integrated application. In this case, AWS services such as Amazon S3 or Amazon Elastic Block Store (EBS) would only see your data encrypted.

Q: Can other AWS services use CloudHSM to store and manage keys?

AWS services integrate with AWS Key Management Service, which in turn is integrated with AWS CloudHSM through the KMS custom key store feature. If you want to use the server-side encryption offered by many AWS services (such as EBS, S3, or Amazon RDS), you can do so by configuring a custom key store in AWS KMS.

Q: Can CloudHSM be used to perform personal identification number (PIN) block translation or other cryptographic operations used with debit payment transactions?

Currently, CloudHSM provides general-purpose HSMs. Over time we may provide payment functions. If this is of interest to you, please [let us know](https://pages.awscloud.com/cloudHSM-contact-us.html).

Q: How does AWS Key Management Service (KMS) compare to AWS CloudHSM?

AWS Key Management Service (KMS) is a multi-tenant, managed service that allows you to use and manage encryption keys. Both services offer a high level of security for your cryptographic keys. AWS CloudHSM provides a dedicated, FIPS 140-2 Level 3 HSM under your exclusive control, directly in your Amazon Virtual Private Cloud (VPC).

Q: When should I use AWS CloudHSM instead of AWS KMS?

You should consider using AWS CloudHSM if you require:

* Keys stored in dedicated, third-party validated hardware security modules under your exclusive control.
* FIPS 140-2 compliance.
* Integration with applications using PKCS#11, Java JCE, or Microsoft CNG interfaces.
* High-performance in-VPC cryptographic acceleration (bulk crypto).

Q: Will my Safenet-based HSMs be retired?

Yes. Gemalto has announced end of life for the HSMs that CloudHSM Classic provides. You must upgrade to the new CloudHSM by April 2020. Please refer to the [CloudHSM Classic FAQ](https://aws.amazon.com/cloudhsm/faqs-classic/) for detailed information. We have developed several resources to assist you in migrating from CloudHSM Classic to the new CloudHSM. You can get started using the [CloudHSM Upgrade Guide](https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Docs/CloudHSMUpgradeGuide-latest.pdf).

Q: How do I get started with CloudHSM?

You can provision a CloudHSM Cluster in the CloudHSM Console, or with a few API calls through the AWS SDK or API. To learn more, please see the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for information about getting started, the [CloudHSM Documentation](https://aws.amazon.com/documentation/cloudhsm/) for information about the CloudHSM API, or the Tools for Amazon Web Services page for more information about the SDK.

Q: How do I terminate CloudHSM service?

You can use the CloudHSM API or SDK to delete your HSMs and stop using the service. Please refer to the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for further instructions.

## Billing

Q: How will I be charged and billed for my use of the AWS CloudHSM service?

You will be charged an hourly fee for each hour (or partial hour) that an HSM is provisioned to a CloudHSM Cluster. A cluster with no HSMs in it is not billed, nor are you billed for our automatic storage of encrypted backups. For more information, please visit the [CloudHSM pricing page](https://aws.amazon.com/cloudhsm/pricing/). Note that network data transfers to and from your CloudHSM instances are charged separately. For more information please review [data transfer pricing](https://aws.amazon.com/ec2/pricing/on-demand/) for EC2.

Q: Is there a Free Tier for the CloudHSM service?

No, there is no free tier available for CloudHSM.

Q: Do charges vary depending on how many users or keys I create on my HSM?

No, the hourly fee, which varies by region, does not depend on how much you use your HSM.

## Provisioning and operations

Q: Are there any prerequisites for signing up for CloudHSM?

Yes. In order to start using CloudHSM there are a few prerequisites, including a Virtual Private Cloud (VPC) in the region where you want CloudHSM service. Refer to the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for more details.

Q: Do I need to manage the firmware on my HSM?

No. AWS manages the firmware on the hardware. Firmware is maintained by a third-party, and every firmware must be evaluated by NIST for FIPS 140-2 Level 3 compliance. Only firmware that has been cryptographically signed by the FIPS key (which AWS does not have access to) can be installed.

Q: How many HSMs should I have in my CloudHSM Cluster?

AWS strongly recommends that you use at least two HSMs in two different Availability Zones for any production workload. For mission-critical workloads, we recommend at least three HSMs in at least two separate AZs. The CloudHSM client will automatically handle any HSM failures and load balance across two or more HSMs transparently to your application.

Q: Who is responsible for key durability?

AWS takes automatic encrypted backups of your CloudHSM Cluster on a daily basis, and additional backups when cluster lifecycle events occur (such as adding or removing an HSM).For the 24-hour period between backups, you are solely responsible for the durability of key material created or imported to your cluster. We strongly recommend ensuring that any keys created are synchronized to at least two HSMs in two different Availability Zones to ensure the durability of your keys. See the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for more detail on verifying key synchronization.

Q: How do I set up a high availability (HA) configuration?

High availability is provided automatically when you have at least two HSMs in your CloudHSM Cluster. No additional configuration is required. In the event an HSM in your cluster fails, it will be replaced automatically, and all clients will be updated to reflect the new configuration without interrupting any processing. Additional HSMs can be added to the cluster via the AWS API or SDK, increasing availability without interrupting your application.

Q: How many HSM instances can be contained in a CloudHSM Cluster?

A single CloudHSM Cluster can contain up to 32 HSMs. Customers can create up to 28 instances, subject to account service limits. The remaining capacity is reserved for internal use, for example when replacing failed HSM instances.

Q: Can I back up the contents of a CloudHSM?

Your CloudHSM Cluster is backed up on a daily basis by AWS. Keys can also be exported (“wrapped”) out of your cluster and stored on-premises as long as they were not generated as “non-exportable”. No other backup options are available at this time, though we expect to provide a more comprehensive on-premises backup capability soon.

Q: Is there an SLA for CloudHSM?

Yes, you can find the service level agreement (SLA) for AWS CloudHSM [here](https://aws.amazon.com/cloudhsm/sla/).

## Security

Q: Do I share my CloudHSM with other AWS customers?

No. As part of the service you receive single-tenant access to the HSM. Underlying hardware may be shared with other customers, but the HSM is accessible only to you.

Q: How does AWS manage the HSM without having access to my encryption keys?

Separation of duties and role-based access control is inherent in the design of CloudHSM. AWS has a limited credential to the HSM that permits us to monitor and maintain the health and availability of the HSM, take encrypted backups, and to extract and publish audit logs to your CloudWatch Logs. AWS is unable to see, access or use your keys, or cause your HSM to perform any cryptographic operation using your keys.

Please see the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for more information on the separation of duties, and the capabilities each class of user has on the HSM.

Q: Can I monitor my HSM?

Yes. CloudHSM publishes multiple CloudWatch metrics for CloudHSM Clusters and for individual HSM instances. You can use the AWS CloudWatch Console, API or SDK to obtain or alarm on these metrics.

Q: What is the ‘entropy source’ (source of randomness) for CloudHSM?

Each HSM has a FIPS-validated Deterministic Random Bit Generator (DRBG) that is seeded by a True Random Number Generator (TRNG) within the HSM hardware module that conforms to SP800-90B. This is a high-quality entropy source capable of producing 20Mb/sec of entropy per HSM.

Q: What happens if someone tampers with the HSM hardware?

CloudHSM has both physical and logical tamper detection and response mechanisms that trigger key deletion (zeroization) of the hardware. The hardware is designed to detect tampering if its physical barrier is breached. HSM instances are also protected against brute-force login attacks. After a fixed number of unsuccessful attempts to access an HSM with Crypto Officer (CO) credentials, the HSM instance will lock the CO out. Similarly, after a fixed number of unsuccessful attempts to access an HSM with Crypto User (CU) credentials, the user will be locked and must be unlocked by a CO.

Q: What happens in case of failure?

Amazon monitors and maintains the HSM and network for availability and error conditions. If an HSM fails or loses network connectivity, the HSM will be automatically replaced. You can check the health of an individual HSM using the CloudHSM API, SDK, or CLI Tools, and you can check the overall health of the service at any time using the [AWS Service Health Dashboard](http://status.aws.amazon.com/).

Q: Could I lose my keys if a single HSM instance fails?

Yes. It is possible to lose keys that were created since the most recent daily backup if the CloudHSM cluster that you are using fails and you are not using two or more HSMs. Amazon strongly recommends that you use two or more HSMs, in separate Availability Zones, in any production CloudHSM Cluster to avoid loss of cryptographic keys.

Q: Can Amazon recover my keys if I lose my credentials to my HSM?

No. Amazon does not have access to your keys or credentials and therefore has no way to recover your keys if you lose your credentials.

Q: How do I know that I can trust CloudHSM?

CloudHSM is built on hardware that is validated at Federal Information Processing Standard (FIPS) 140-2 Level 3. You can find information about the FIPS 140-2 Security Profile for the hardware used by CloudHSM, and the firmware it runs, at our [compliance page](https://docs.aws.amazon.com/cloudhsm/latest/userguide/compliance.html).

Q: Does the CloudHSM service support FIPS 140-2 Level 3?

Yes, CloudHSM provides FIPS 140-2 Level 3 validated HSMs. You can follow the procedure in the [CloudHSM User Guide](https://aws.amazon.com/documentation/cloudhsm/) under [Verify the Authenticity of Your HSM](https://docs.aws.amazon.com/cloudhsm/latest/userguide/verify-hsm-identity.html) to confirm that you have an authentic HSM on the same model hardware specified in the NIST Security Policy described in the previous question.

Q: How do I operate a CloudHSM in FIPS 140-2 mode?

CloudHSM is always in FIPS 140-2 mode. This can be verified by using the CLI tools as documented in the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) and running the getHsmInfo command, which will indicate the FIPS mode status.

Q: Can I get a history of all CloudHSM API calls made from my account?

Yes. [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) records AWS API calls for your account. The AWS API call history produced by CloudTrail lets you perform security analysis, resource change tracking, and compliance auditing. Learn more about CloudTrail at the CloudTrail home page, and turn it on via [CloudTrail's AWS Management Console](https://console.aws.amazon.com/cloudtrail/home).

Q: Which events are not logged in CloudTrail?

CloudTrail does not include any of the HSM device or access logs. These are provided directly to your AWS account via CloudWatch Logs. See the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for more details.

## Compliance

Q: Which AWS compliance initiatives include CloudHSM?

Please refer to the [AWS Compliance](https://aws.amazon.com/compliance/) site for more information about which compliance programs cover CloudHSM. Unlike other AWS services, compliance requirements regarding CloudHSM are often met directly by the FIPS 140-2 Level 3 validation of the hardware itself, rather than as part of a separate audit program.

Q: Why is FIPS 140-2 Level 3 important?

FIPS 140-2 Level 3 is a requirement of certain use cases, including document signing, payments, or operating as a public Certificate Authority for SSL certificates.

Q: How can I request compliance reports that include CloudHSM in scope?

You can request compliance reports through your Business Development representative. If you don’t have one, you can request one [here](https://pages.awscloud.com/compliance-contact-us.html).

## Performance and capacity

Q: How many crypto operations per second can CloudHSM perform?

The performance of the individual HSMs varies based on the specific workload. The table below shows approximate single-HSM performance for several common cryptographic algorithms. You can create up to 28 HSM instances in each CloudHSM Cluster, so you can achieve up to ~28x the performance of the table listed below per cluster. Performance can vary based on exact configuration and data sizes, so we encourage load testing your application with CloudHSM to determine exact scaling needs.

|  |  |
| --- | --- |
| RSA 2048-bit sign/verify | 1,100/sec |
| EC P256 | 315 point mul/sec |
| AES 256 | 300Mb/sec full-duplex bulk encryption |
| 2048-bit RSA Key Generation | ~0.5/sec |
| Random Number Generation (CSPRNG) | 20Mb/sec |

Q: How many keys can be stored on a CloudHSM instance?

A CloudHSM cluster can store approximately 3,300 keys of any type or size.

## AWS CloudHSM for Oracle TDE

Q: Does CloudHSM support Amazon RDS Oracle TDE?

No. Amazon RDS Oracle TDE is not supported; however, Oracle TDE is supported for Oracle Databases (11g and 12c) operating in EC2. See the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/) for additional details. You can also use AWS Key Management Service (KMS) with [Custom Key Store](https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html) to secure Amazon RDS data using keys generated and stored in your AWS CloudHSM cluster.

## AWS CloudHSM client, API and SDK

Q: What is the CloudHSM Client?

The CloudHSM Client is a software package supplied by AWS that allows you and your applications to interact with CloudHSM Clusters.

Q: Does the CloudHSM Client give AWS access to my CloudHSM Cluster?

No. All communication between the client and your HSM is encrypted end to end. AWS cannot see or intercept this communication, and has no visibility into your cluster access credentials.

Q: What are the CloudHSM Command Line Interface (CLI) Tools?

The CloudHSM Client comes with a set of CLI tools that allow you to administrate and use the HSM from the command line. Linux and Microsoft Windows are supported today. Support for Apple macOS is on our roadmap. These tools are available in the same package as the CloudHSM Client.

Q: How can I download and get started with the CloudHSM Command Line Interface Tools?

You’ll find instructions in the [CloudHSM User Guide](https://docs.aws.amazon.com/cloudhsm/latest/userguide/).

Q: Do the CloudHSM CLI Tools provide AWS with access to the contents of the HSM?

No. The CloudHSM Tools communicate directly with your CloudHSM Cluster via the CloudHSM Client over a secured, mutually authenticated channel. AWS cannot observe any communication between the client, tools, and HSM, it is encrypted end-to-end.

Q: On what operating systems can I use the CloudHSM Client and CLI Tools?

Multiple Linux flavors (modern versions of Amazon Linux, Redhat, Centos, and Ubuntu) and Microsoft Windows are supported today. Support for Apple macOS is on our roadmap. Please let us know if there are other operating systems on which you would like to use the CloudHSM Client and CLI Tools.

Q: What are the network connectivity requirements for using the CloudHSM Command Line Interface Tools?

The host on which you are running the CloudHSM Client and/or using the CLI Tools must have network reachability to all of the HSMs in your CloudHSM Cluster.

Q: What can I do with the CloudHSM API & SDK?

You can create, modify, delete, and obtain the status of CloudHSM Clusters and HSMs. What you can do with the AWS CloudHSM API is limited to operations that AWS can perform with its restricted access. The API cannot access the contents of the HSM or modify any users, policies, or other settings. To learn more, please see the [CloudHSM Documentation](https://aws.amazon.com/documentation/cloudhsm/) for information about the API, or the [Tools for Amazon Web Services](https://aws.amazon.com/tools/) page for more information about the SDK.

## Migrating to new CloudHSM

Q: How should I plan my migration to AWS CloudHSM?

Start by ensuring that the algorithms and modes you require are [supported by CloudHSM](https://docs.aws.amazon.com/cloudhsm/latest/userguide/pkcs11-library.html). Your account manager can submit feature requests to us if needed. Next, determine your key rotation strategy. Suggestions for common use cases are in the next Q/A. We have also published an in-depth [migration guide for CloudHSM](https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Docs/CloudHSMUpgradeGuide-latest.pdf). You're now ready to [get started](https://docs.aws.amazon.com/cloudhsm/latest/userguide/getting-started.html) with the new CloudHSM.

Q: How can I rotate my keys?

Your rotation strategy will depend on the type of application. Common examples are below.

* Private keys for signing: Generally the private key on the HSM corresponds to an intermediate certificate, which is in turn signed by an offline enterprise root. You will rotate keys by issuing a new intermediate certificate. Create a [new private key and generate the corresponding CSR using OpenSSL](https://docs.aws.amazon.com/cloudhsm/latest/userguide/ssl-offload-import-or-generate-private-key-and-certificate.html) on CloudHSM. Next, sign the CSR with the same offline enterprise root. You may have to register this new certificate with any partners who do not automatically verify the entire certificate chain. Moving forward, you would sign all new requests (such as for documents, code or other certificates) with the new private key, corresponding to the new certificate. You can continue to verify signatures from the original private key using the corresponding public key. No revocation is necessary. This process is analogous to the process you would follow to retire or archive a signing key.
* Oracle Transparent Data Encryption: You can transfer your wallet by first switching from a hardware keystore (your original HSM) to a [software keystore](https://docs.oracle.com/cloud/latest/db121/ASOAG/asotrans_gen.htm#ASOAG10408), and then back to a [hardware keystore](https://docs.aws.amazon.com/cloudhsm/latest/userguide/oracle-tde-configure-database-and-generate-master-key.html) (the new CloudHSM).
* Symmetric key for envelope encryption: Envelope encryption refers to the key architecture where one key on the HSM encrypts/decrypts many data keys on the application host. You likely already have a key rotation process in place to go through and decrypt the data keys with the old wrapping key and re-encrypt them with the new wrapping key. The only difference during migration will be that the new wrapping key will be created and used on CloudHSM instead of your original HSM. If you do not already have a key rotation tool and process in place, you will need to create one.

Q: What if I can't rotate my keys?

Each application and use case is different. Solutions to common scenarios are discussed in the [migration guide for CloudHSM](https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Docs/CloudHSMUpgradeGuide-latest.pdf). For additional questions, open a support case with details of your application, the type of HSM you are using today, the type of keys you are using, and whether these keys are exportable or not. We will help you determine an appropriate migration path.

## Support and maintenance

Q: How is routine maintenance performed on HSM instances?

AWS’ routine maintenance procedure for CloudHSM is designed to avoid simultaneous downtime in multiple AZs in the same region.

AWS monitors and maintains the HSM instances. We may need to remove an HSM instance from service for upgrade, replacement, or test purposes. Such operations are expected to take less than twenty minutes in the case of a replacement, and should not interfere with the performance of your CloudHSM Cluster under normal circumstances. An application that is actively using a specific HSM in the cluster when it is replaced may experience a momentary disruption while the CloudHSM Client retries the operation on a different HSM in the cluster.

AWS will not perform routine maintenance on HSMs in multiple AZs within the same region within the same 24-hour period.

In unforeseen circumstances, it is possible that AWS might perform emergency maintenance without prior notice. AWS will try to avoid this situation, as well as situations where emergency maintenance is performed within the same 24-hour period on HSMs in multiple AZs in the same region.

AWS strongly recommends that you use CloudHSM Clusters with two or more HSMs in separate Availability Zones to avoid any potential disruption.

Q: I am having a problem with CloudHSM. What do I do?

Contact [AWS Support](https://aws.amazon.com/support/).