AWS CloudHSM AND AWS Key Management Service

AWS Black Belt Tech Webinar 2015 (旧マイスターシリーズ)

アマゾンデータサービスジャパン株式会社
ソリューションアーキテクト 布目 拓也
セキュリティコンサルタント 高田 智己

2015.07.29

amazon web services

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

CloudHSMとは

- AWS上のハードウェアセキュリティモジュール(HSM)
- 鍵管理と暗号化処理のためのセキュアデバイス
- 秘密鍵の強固な保護
  - 物理的に鍵にアクセスできない
  - アプライアンスの管理者（AWS）は鍵にアクセス出来ない
- セキュリティ標準に準拠する第三者認証

HSM

AWS CloudHSMがサポートしているリージョン

- 2015/7現在
  - 米国東部（バージニア北部）
  - 米国西部（オレゴン）
  - 欧州（アイルランド）
  - 欧州（フランクフルト）
  - アジアパシフィック（シドニー）
  - アジアパシフィック（シンガポール） **- New !**
  - アジアパシフィック（東京） **- New !**

AWS KMSとCloud HSMの違い

	AWS CloudHSM	AWS Key Management Service
専有性	VPCにお客様専用のハードウェアデバイス（ Safe Net Luna SA 7000 HSM)をインストール。	マルチテナントのマネージドサービス
可用性	可用性と耐久性はお客様が管理	高可用性、耐久性の高い鍵保管用ストレージと鍵管理
Root of trust	“root of trust”はお客様が管理	“root of trust”はAWSが管理
コンプライアンス	FIPS 140-2 レベル 2及び情報セキュリティ国際評価基準 EAL4+標準に準拠。耐タンパー性を備える。CloudTrailにも対応。	CloudTrailとの統合による監査機能
操作	現在のところ管理コンソール対応無し（CloudHSM CLI等CLIで操作）	管理コンソール、SDK、AWS CLI
サードパーティ製品	EBS用SafeNet ProtectV ボリューム暗号化、Apache、Microsoft SQL Server（透過的データ暗号化）等	（カスタムソフトウェア。AWS SDKは提供）
AWSサービス	Redshift, RDS(Oracle TDE)	S3, EBS, RDS(全エンジン）,Redshift, Elastic Transcoder, WorkMail , EMRFS
暗号化機能	共通及び公開鍵暗号に対応	現在のところ共通鍵暗号のみ
コスト	概ね固定費	従量課金

サポートしているサービスの例

- CloudHSM for RDS Oracle TDE
- Redshift Encryption
- EBS Volume Encryption with SafeNet ProtectV & KeySecure
- Database Encryption (non-RDS, Oracle/MS SQL TDE)
- Custom Software Applications

サポートされている暗号化アルゴリズム

サポートしている暗号アルゴリズム	
暗号化手段	Full Suite B support
	Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves
	Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
	Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC
	Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)
サポートしているAPI	
暗号化API	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL

http://www.safenet-inc.com/data-encryption/hardware-security-modules-hsms/luna-hsms-key-management/luna-sa-network-hsm/

SafeNet Luna SA 7000のパフォーマンス

Algorithm	Transactions/second
RSA-1024	7000
RSA-2048	1200
ECC P256	2000
ECIES	300
AES-GCM	3700

実際の処理量はネットワークのレイテンシー等により変化するので事前の検証が必要です。

http://www.safenet-inc.com/data-encryption/hardware-security-modules-hsms/luna-hsms-key-management/luna-sa-network-hsm/

CloudHSMが選ばれる理由

- **コントロール**
  - 暗号鍵の完全な管理。AWSはキーマテリアルにアクセス不可
  - 暗号鍵の利用に対するきめの細かいコントロール

- **コンプライアンス対応**
  - FIPS 140-2 level 2 certification
  - Common Criteria EAL-4 certification

- **パフォーマンス**
  - AWS上のアプリケーションにとってローカルに置かれるCloudHSM

コントロール - 安全な鍵管理

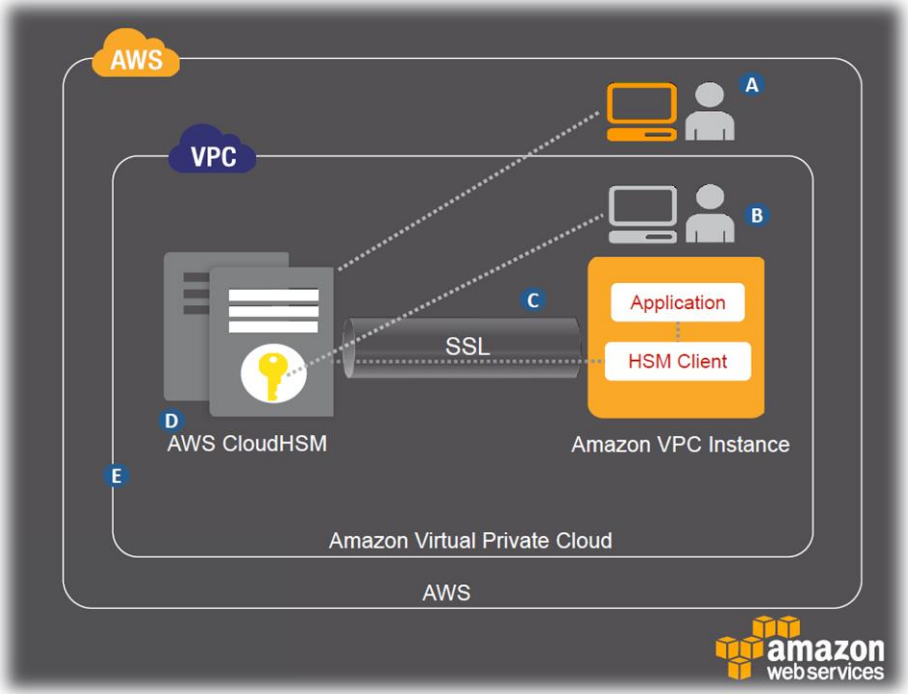
A. AWSはHSMアプライアンスを管理しますが、お客様の鍵にはアクセスしません。

B. お客様自身でHSMを初期化・設定します。お客様は、自ら鍵の管理・制御が可能です。

C. 閉域ネットワークのためAWSの負荷によらず、アプリケーションの性能を向上させることができます。

D. 厳重に管理された鍵保管庫は、複数のリージョン及びAZに設置できます。

E. CloudHSMは、顧客のVPCに設置でき、他のネットワークからは隔離されます。



amazon web services

コンプライアンス対応

- 次のような要件が求められるケース
  - PCI　DSSやその他の特定の縦断的なセキュリティ標準
  - 政府のワークロード (US, Canada,等)
  - エンタープライズ企業で増加しているFIPS認可要求ポリシー

- CloudHSMはSafeNet Luna SAアプライアンスを提供
  - FIPS 140-2 Level 2 validation (Luna SA自体はLevel3)
  - Common Criteria EAL-4 validation

パフォーマンス

- CloudHSMをEC2の近くのVPCに配置することにより、ネットワークレイテンシーが低減。HSMを使用するアプリケーションのパフォーマンスを向上させることが可能。

- オンプレミスにHSMを持つ場合
  - HSMアクセスが必要なAWSアプリケーションはVPNまたはDX経由でオンプレミスのHSMにアクセスする必要がある
  - レイテンシーと可用性の観点から、CloudHSMが望ましい
  - CloudHSMはSafeNet Luna SA HSM アプライアンスと互換性があるため併用することも可能

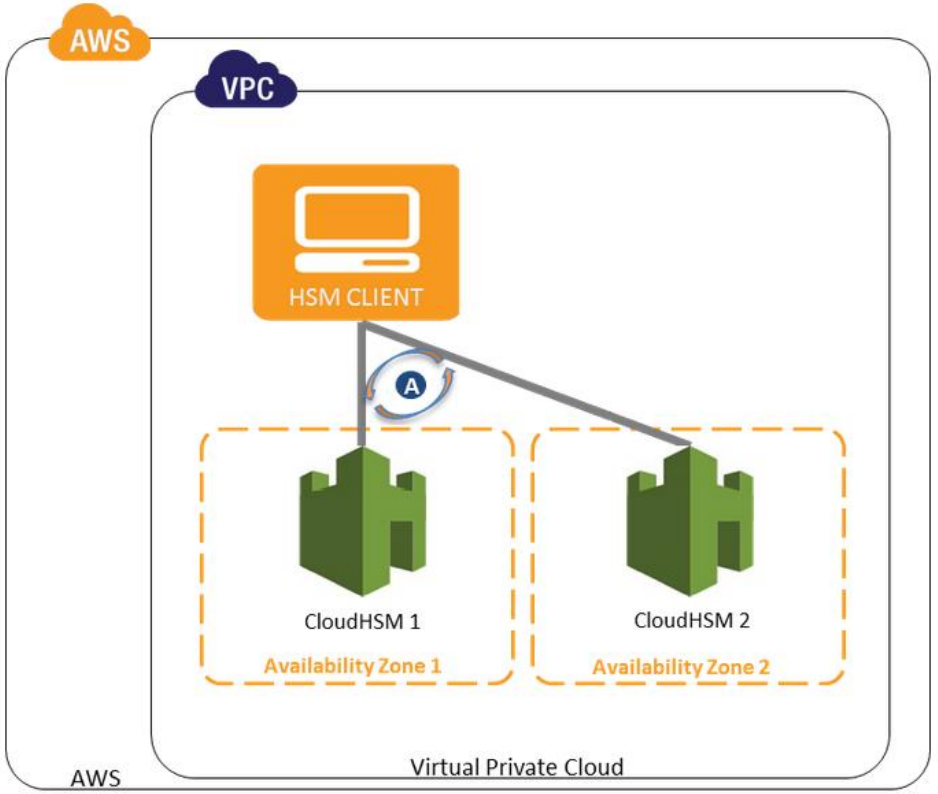
HSMの運用

- 各HSMはお客様専有で割り当て
  - アプライアンスの共有やパーティショニングは行わない
- お客様にて冗長化を管理する必要がある
  - SafeNet クライアントは複数のHSM間のレプリケーションをハンドル(最大16)
  - SafeNet クライアントで利用可能なHSMを跨ったロードバランスが可能
- HSMへのコントロールアクセスはパスワード認証
  - PED (Pin Entry Devices) は現時点では未サポート
- AWSは物理デバイスとネットワークインフラのモニタリングと管理を行う

AWS CloudHSMの冗長化

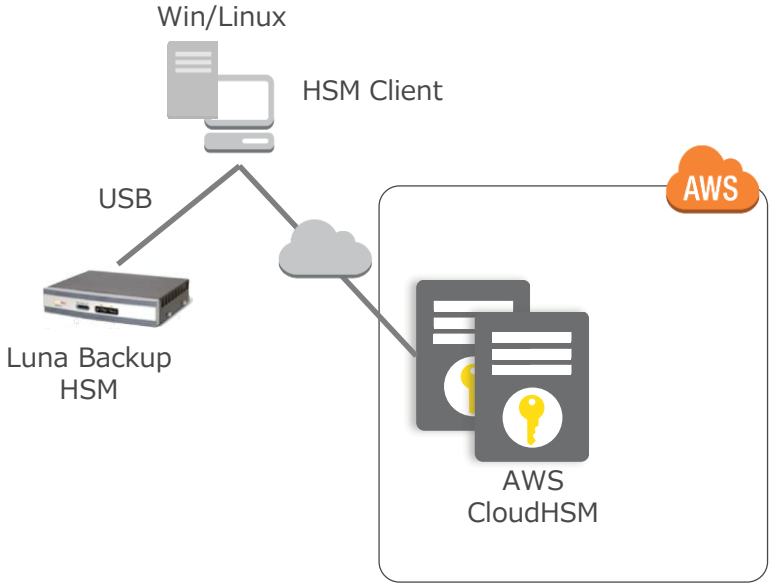
A. HSMクライアントソフトウェアは、複数のAZにまたがる2つ以上のCloudHSMインスタンスの間でリクエストのロードバランスを取ることができます。

- CloudHSMの冗長化は利用者が行う必要があります。
- CloudHSMに保存されたキーを、参加しているその他のHSMに、自動的にかつ安全に複製できます。
- 可用性と耐久性の高い構成にするには、複数のアベイラビリティーゾーンの間で少なくとも2つのCloudHSMインスタンスを使用することをお勧めします。



外部へのバックアップとリストア

- On-Premisesも含むHA構成外へのバックアップには別売りのLuna Backup HSMを利用
- Luna Backup HSMはLuna SAと同程度のセキュリティレベルにあるポータブルアプライアンス
- USBでHSM Clientとして接続しているクライアントマシーンに接続しバックアップ・リストアを行う



http://docs.aws.amazon.com/ja_jp/cloudhsm/latest/userguide/cloud-hsm-backup-restore.html

http://www.safenet-inc.com/WorkArea/DownloadAsset.aspx?id=8589948302

監査

- CloudTrail
  - リソース変更の追跡
  - セキュリティとコンプライアンスのためのアクティビティに対する監査
  - 全てのCloudHSM API コールをレビュー

- Syslog
  - HSMアプライアンスに対するオペレーションを監査
  - ユーザーのSyslog収集サーバにログを送信

CloudTrailのサンプル


```
{
   "eventVersion": "1.02",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAJZMJFOOK2OKHUIHB6",
      "arn": "arn:aws:iam::26883621xxxx:user/CloudHSM-LAB",
      "accountId": "26883621xxxx",
      "accessKeyId": "AKIAJ52HATLZJZF5xxxx",
      "userName": "CloudHSM-LAB"
   },
   "eventTime": "2015-07-21T23:55:37Z",
   "eventSource": "cloudhsm.amazonaws.com",
   "eventName": "CreateHsm",
   "awsRegion": "ap-northeast-1",
   "sourceIPAddress": "52.69.184.xx",
   "userAgent": "Boto/2.38.0 Python/2.7.9 Linux/3.14.27-
25.47.amzn1.x86_64",
   "requestParameters": {
      "iamRoleArn":
"arn:aws:iam::26883621xxxx:role/CloudHSM-LAB-
CloudHsmRole-T5SM2ECQO71A",
"sshKey": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCuiCvTNAvpO0xFbQ9
xM+nT7SBpH9i72O182wlxjPhWUNfz1cC64vWgQcXq
j ec2-user@ip-10-0-0-86",
      "syslogIp": "10.0.0.86",
      "subscriptionType": "PRODUCTION",
      "subnetId": "subnet-b6c1xxxx",
      "clientToken": "a2e1c5e666b6454e89b42bf3xxxxxxxx"
   },
   "responseElements": {
      "hsmArn": "arn:aws:cloudhsm:ap-northeast-
1:26883621xxxx:hsm-ad6a552c"
   },
   "requestID": "fac88b27-3003-11e5-a6c8-1d9382ab7fc3",
   "eventID": "23863c70-fbb2-4648-a894-c24eb8903264",
   "eventType": "AwsApiCall",
   "recipientAccountId": "26883621xxxx"
}
```

Syslogのサンプル

```
Jul 22 01:02:25 hsm-7-3-1-10 lunash [30233]: info : 0 : Lush user login : manager : 192.168.0.194/48782
Jul 22 01:02:25 hsm-7-3-1-10 lunash [30233]: info : 0 : Command: package list  : manager : 192.168.0.194/48782
Jul 22 01:02:27 hsm-7-3-1-10 lunash [30233]: info : 0 : Command: hsm show  : manager : 192.168.0.194/48782
Jul 22 01:02:29 hsm-7-3-1-10 lunashlast message repeated 2 times
Jul 22 01:02:29 hsm-7-3-1-10 lunash [30269]: info : 0 : Lush user login : manager : 192.168.0.194/48783
Jul 22 01:02:30 hsm-7-3-1-10 lunash [30269]: info : 0 : Command: package list  : manager : 192.168.0.194/48783
Jul 22 01:02:32 hsm-7-3-1-10 lunash [30269]: info : 0 : Command: package list  : manager : 192.168.0.194/48783
Jul 22 01:02:34 hsm-7-3-1-10 lunash [30269]: info : 0 : Command: hsm init -label adsjhsm2 -domain * -password * -force :
manager : 192.168.0.194/48783
Jul 22 01:02:36 hsm-7-3-1-10 Luna PED Client[1958]: info : 0 : Address trying to connect to Admin Service is 127.0.0.1
Jul 22 01:02:36 hsm-7-3-1-10 Luna PED Client[1958]: info : 0 : Admin query command received.
Jul 22 01:02:36 hsm-7-3-1-10 sysstatd: Luna System State Server - OOS Errors: 20,100!
Jul 22 01:02:38 hsm-7-3-1-10 Luna PED Client[1958]: info : 0 : Address trying to connect to Admin Service is 127.0.0.1
Jul 22 01:02:38 hsm-7-3-1-10 Luna PED Client[1958]: info : 0 : Admin query command received.
Jul 22 01:02:40 hsm-7-3-1-10 Luna PED Client[1958]: info : 0 : Address trying to connect to Admin Service is 127.0.0.1
Jul 22 01:02:40 hsm-7-3-1-10 Luna PED Client[1958]: info : 0 : Admin query command received.
Jul 22 01:02:40 hsm-7-3-1-10 lunash [30269]: info : 0 : Command: ntls bind eth0 -force : manager : 192.168.0.194/48783
Jul 22 01:02:40 hsm-7-3-1-10 NTLS[30541]: info : 0 : SA command processor configured with 50 worker threads
Jul 22 01:02:40 hsm-7-3-1-10 NTLS[30541]: info : 0 : "Luna SA 5.0 Command Processor" module version 2.0 loaded
```

CloudHSM CLIツール

- プロビジョニングと削除
  - HSMのプロビジョニングと初期化、他のHSMからの鍵コピーを容易に実施可能
- HSMの容易な管理を実現
  - CLIを利用した自動化により運用負荷を軽減
- HA構成設定の簡素化
  - 容易にHSMのHA設定構成の設定と管理が可能
  - アプライアンスシェルで直接インタラクティブに行う場合9ステップの操作が必要
  - CLIの場合、create-hapg, add-hsm-to-hapgの2ステップ (HSM毎に実施)
- ソースコードはオープンソースとして公開

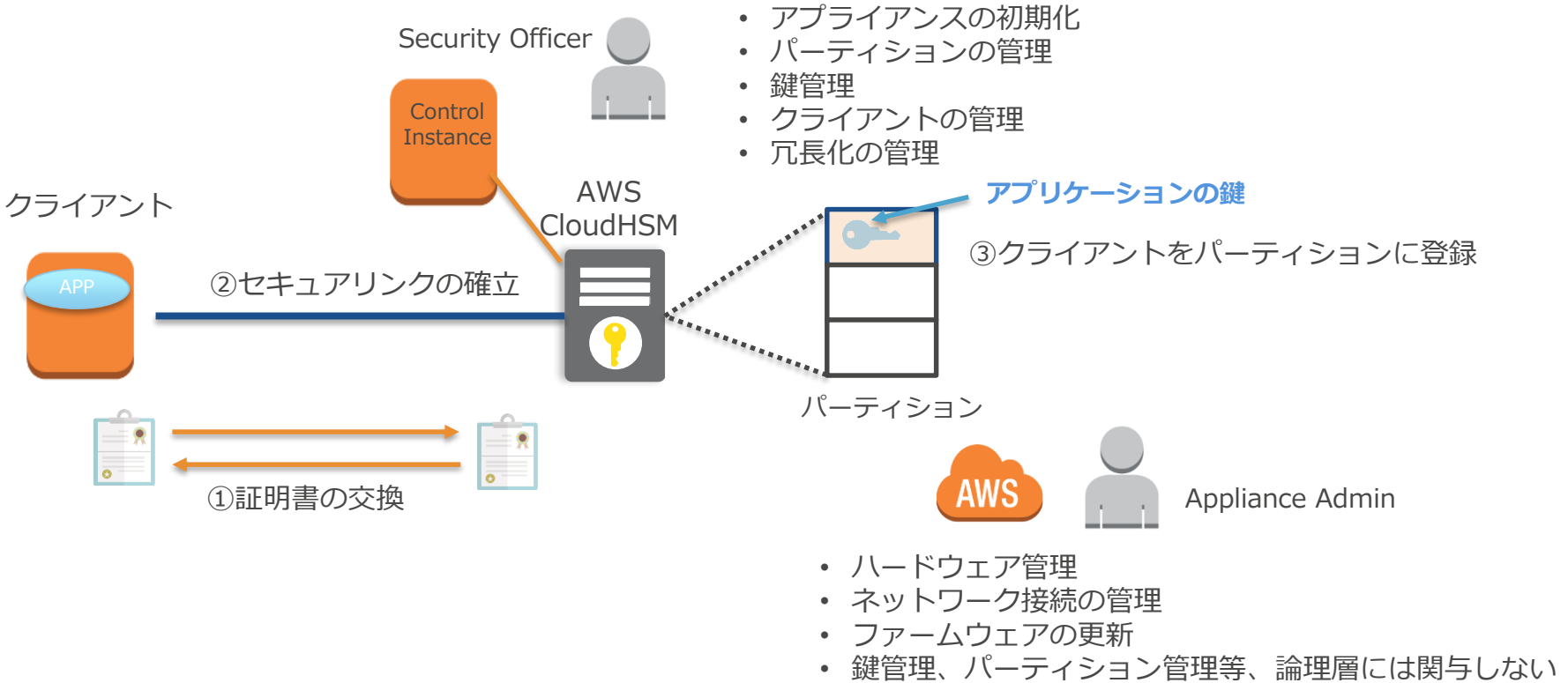
CloudHSM パブリック APIとSDK

- パブリックAPI経由でセルフサービスのプロビジョニングと管理をサポート
  - CreateHSM / DeleteHSM ：HSMのプロビジョニングと削除
  - ModifyHSM :ネットワーク構成の変更とsyslogフォワーディングの設定
  - ListHsms / DescribeHsm :プロビジョニング済みHSM情報の表示
  - ListAvailableZones 利用可能なCloudHSMのキャパシティを表示

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

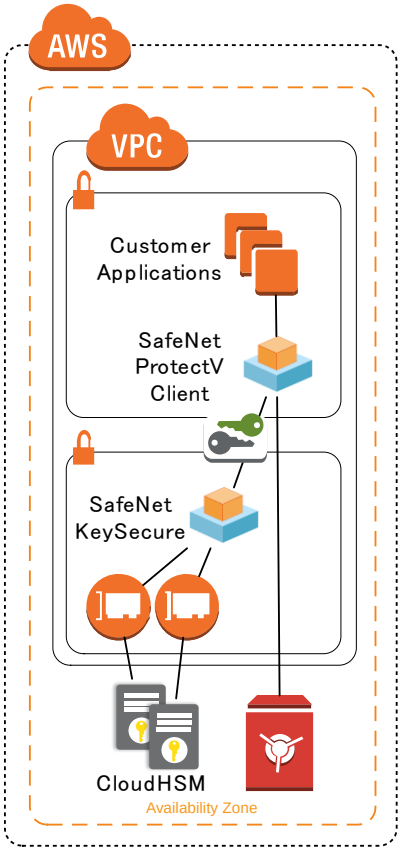
CloudHSM登場人物概要図



- アプライアンスの初期化
- パーティションの管理
- 鍵管理
- クライアントの管理
- 冗長化の管理

- ハードウェア管理
- ネットワーク接続の管理
- ファームウェアの更新
- 鍵管理、パーティション管理等、論理層には関与しない

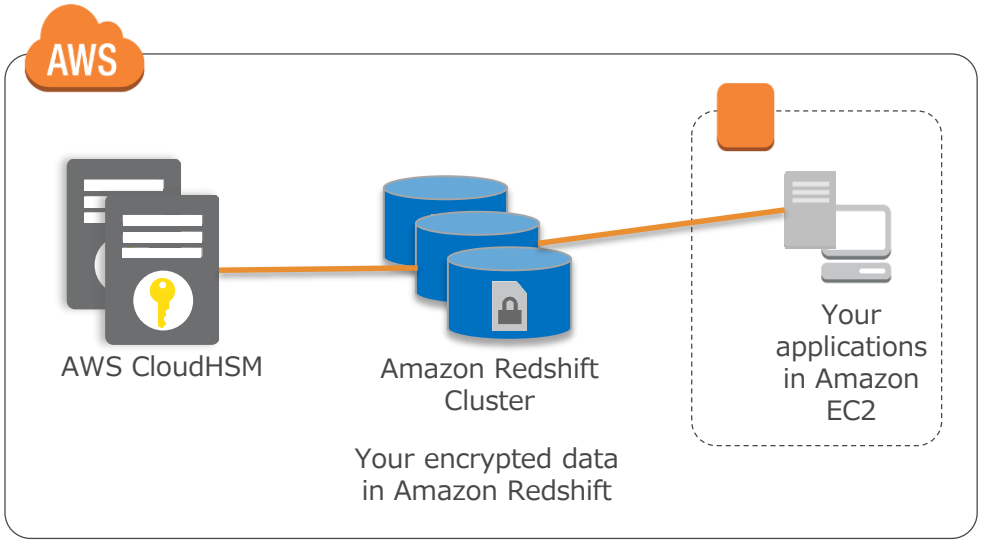
EBSボリューム暗号化



- マスターキーはCloudHSMに保管
- SafeNet ProtectV と KeySecureを利用
- ProtectVクライアントが導入されたインスタンスをKeySourceで認証
- ProtectV クライアントがEBSボリュームに対する全てのI/Oを暗号化
(AES256を利用)

Redshift 暗号化

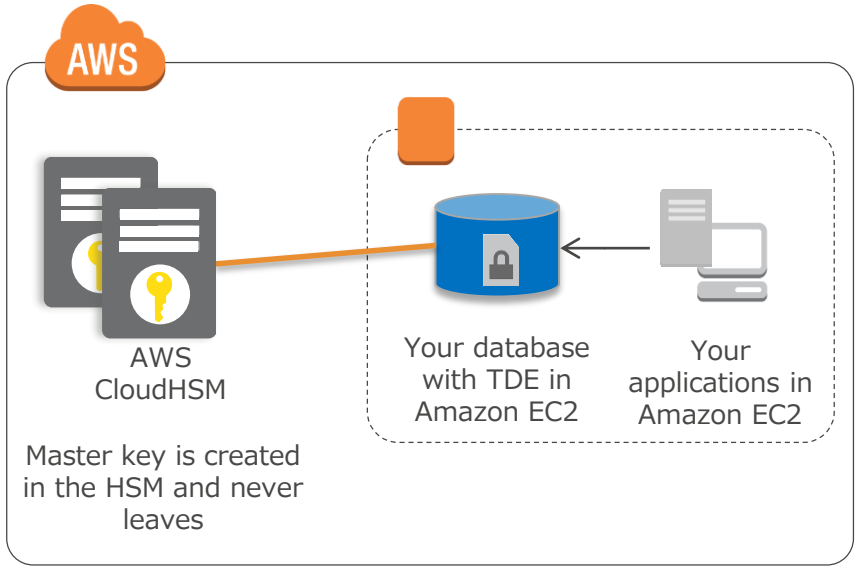
- クラスターマスターキー を CloudHSMに保管
- ダイレクトインテグレーション – クライアントソフトウェアは不要



- 通信路はSSLで、保存済みデータはAES256で暗号化
- HSM がクラスターキーを生成
- クラスターキーはHSMに残る
- クラスタはデータベースキーを作成し、HSMのクラスターキーで暗号化して保管
- クラスタは必要に応じてデータベースキーを復号し、メモリ上に保存

データベース暗号化(RDS以外)

- EC2上のお客様管理データベース
  - Oracle 11g & 12c での Transparent Data Encryption (TDE)
  - Microsoft SQL Server 2008 & 2012 でのTDE
  - マスターキーをCloudHSMに保管



CloudHSM for RDS Oracle TDE

- RDS OracleでのTransparent data encryptionサポート
- マスターの暗号鍵をCloudHSMに保管
- 2つ以上のHSMを利用した高可用性構成をサポート
- HSMあたり20インスタンスまで対応可能

2015年7月現在、東京リージョン、シンガポールリージョンでは未サポート

カスタムアプリケーション

- セキュアなアプリケーション開発のためのアーキテクチャルなビルディングブロックを提供

- バックエンドにHSMを利用するスタンダードライブラリを利用
  - PKCS#11, JCA/JCE, Microsoft CAPI/CNG/EKM

- コードサンプルと詳細はCloudHSMユーザーガイドを参照

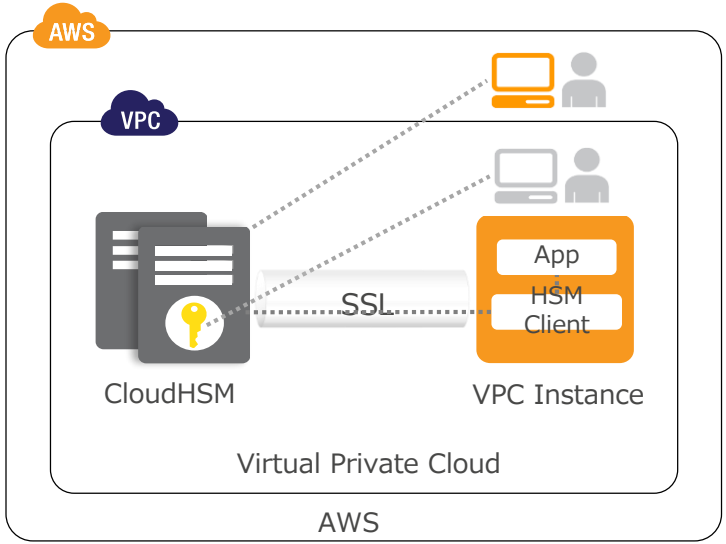
ユースケース例

- お客様のユースケース:
  - オンプレミスでHSMを利用しているエンタープライズ企業のCloud移行
  - 高保証サービスとコンプライアンス準拠を提供したいスタートアップ企業
  - オンプレミスではHSMを利用していないアプリケーションでもCloudに移行する際にはHSMを使いたいと考えているエンタープライズ企業

- アプリケーション例:
  - オブジェクト暗号化
  - デジタル著作権管理(DRM)
  - 文書の署名、セキュアなドキュメント管理とセキュアなドキュメントリポジトリ
  - 決済や金融アプリケーションとそのトランザクション処理
  - 特権ユーザー管理
  - 認証局(CA)

お客様例: Netflix

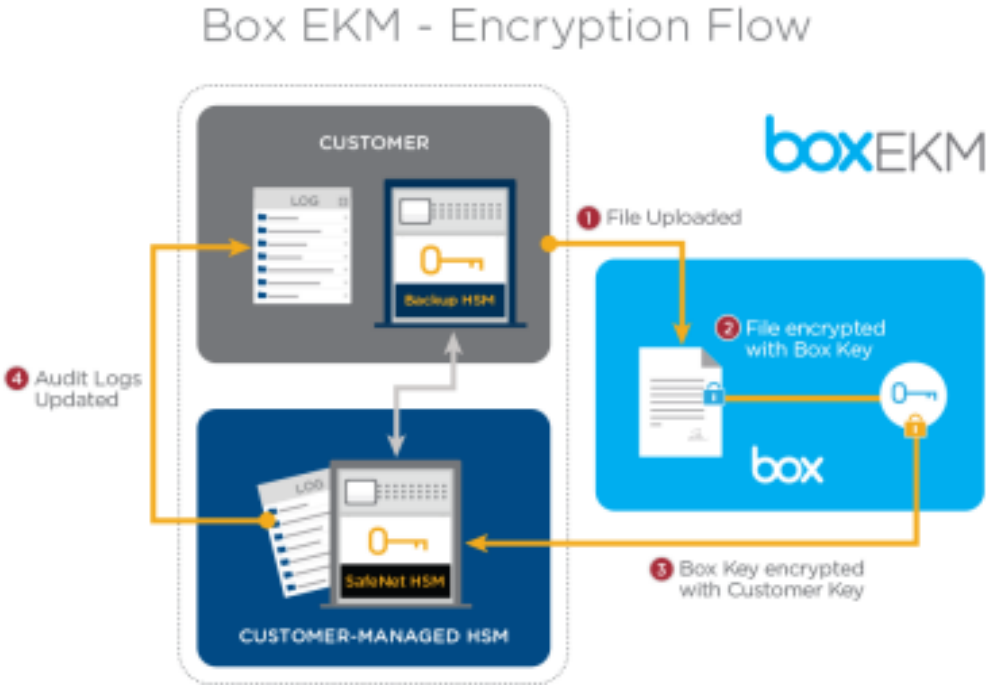
- ゴール
  - データセンターの依存性と複雑性を削除
  - 信頼性とパフォーマンスの強化
- アプローチ
  - リージョン/環境ごとにHSMを配置
  - データセンターのSafeNet DataSecureからCloudHSMへのマイグレーション
  - データセンターをディスコン
- 結果
  - 3つのリージョンでAWS Cloud HSMアプライアンスを利用
  - より低いレイテンシーと高いセキュリティ
  - オンプレミスデータセンターベースのHSMと鍵管理システムを削除
  - 当初の予定より33%のコスト削減



http://www.slideshare.net/AmazonWebServices/encryption-and-key-management-in-aws-sec304-aws-reinvent-2013

お客様例：Box (EKM)

- 企業でBoxを利用したコンテンツ管理ならびにコラボレーションツールを利用可能にするサービスで、CloudHSMを使用。



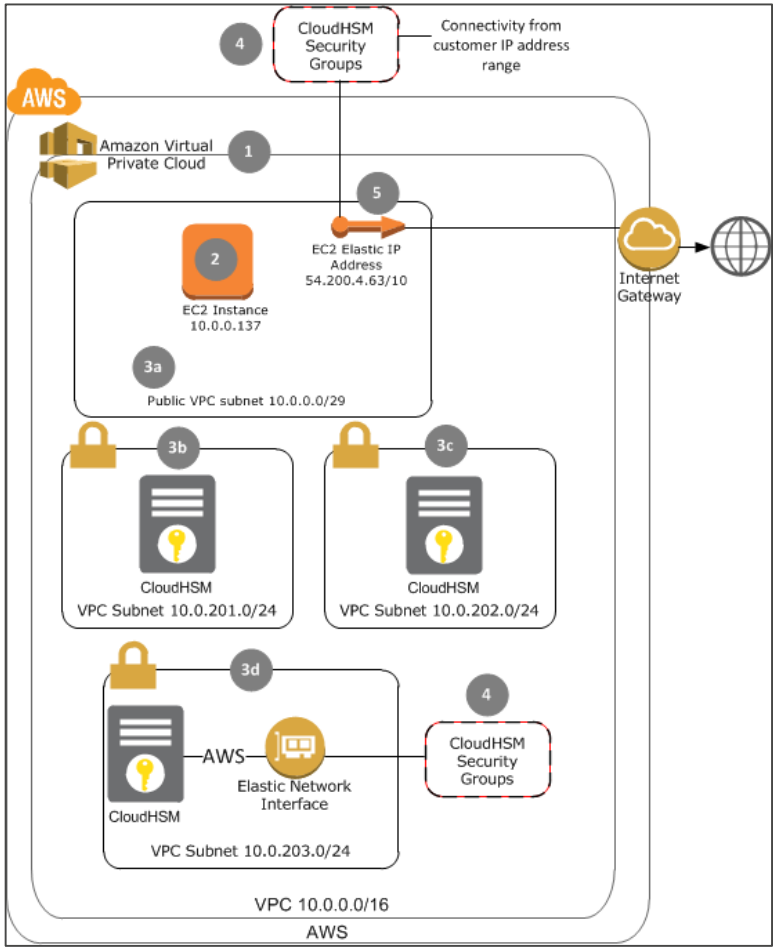
http://aws.typepad.com/aws_japan/2015/02/box-enterprise-key-management-powered-by-aws-cloudhsm.html

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

利用開始方法

- ベースの環境の構築
  - VPC/Subnet/SG/IAM/Control Instance
  - CloudFormationによる環境構築
    OR
  - マニュアルによる環境構築
- CloudHSMのCLI Toolの導入
- CLI ToolよりCloudHSMのProvisioning
- CoudHSMの初期化・構成



CloudFormationによるインフラ構築

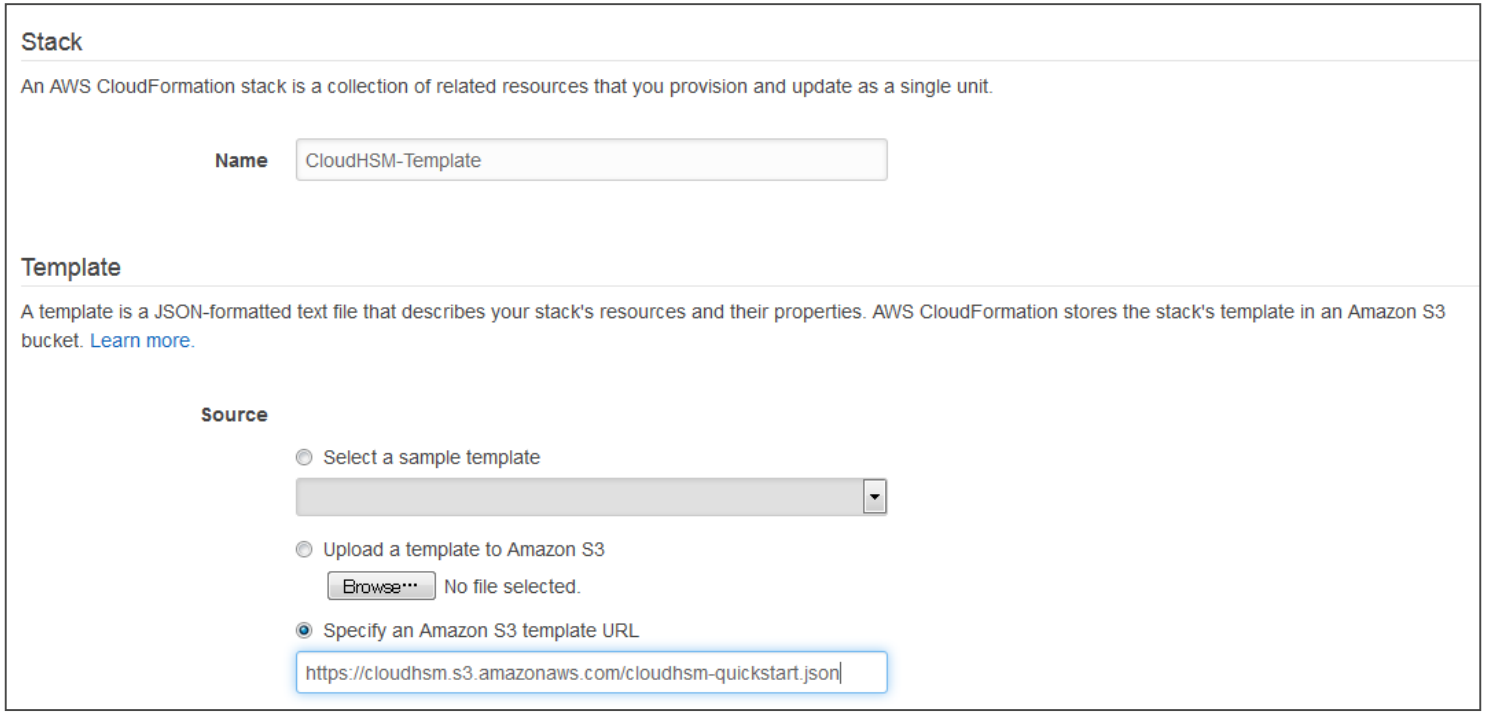
- 以下のURLでCloudHSM用のテンプレートが提供されています。
  https://cloudhsm.s3.amazonaws.com/cloudhsm-quickstart.json

- テンプレートには東京リージョンを含む各リージョンの定義が含まれています。

- CloudFormationのテンプレートで作られるもの
  - ネットワーク：VPC, Subnet
  - Control Instance及びCloudHSM用のSecurity Group
  - CloudHSM用のIAM Role
  - Control Instance

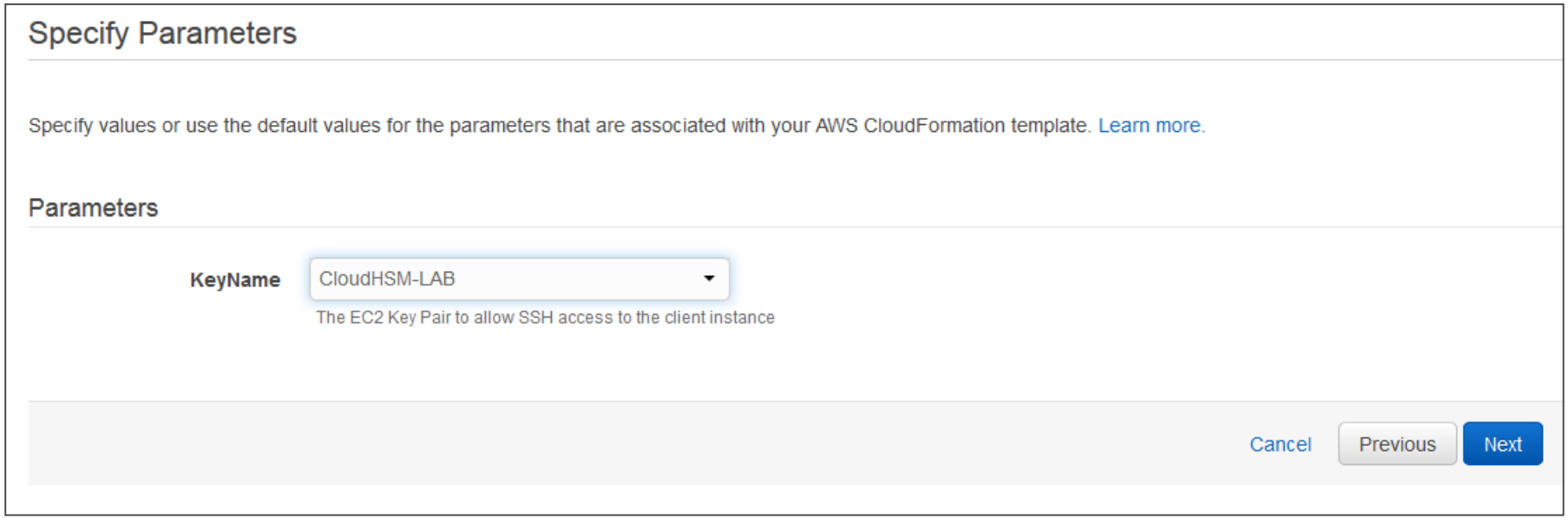
CloudFormationによるインフラ構築

- CloudFormationでテンプレートを実行します



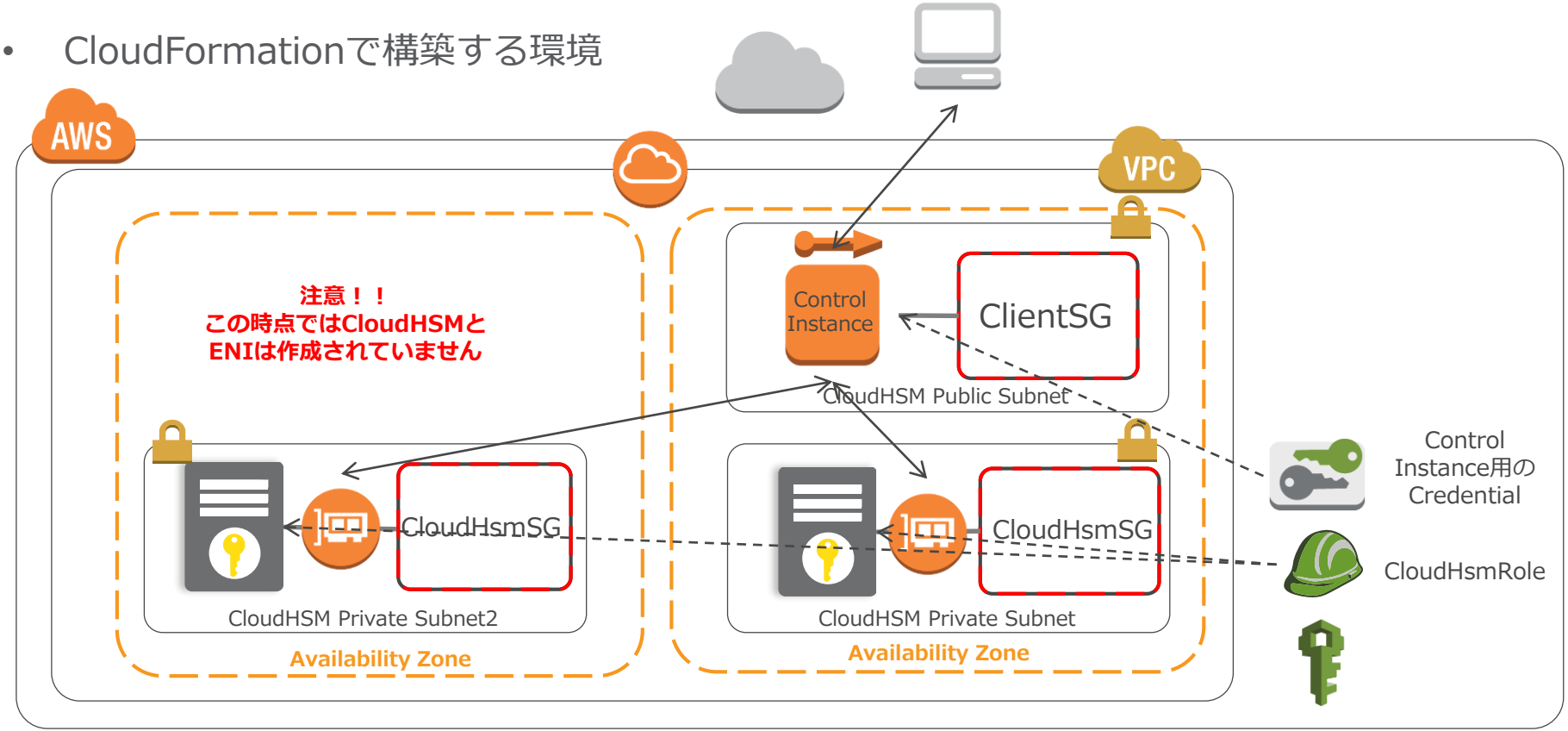
CloudFormationによるインフラ構築

- EC2（Control Instance）が利用するキーペアを指定します。キーペアは予め作成しておいてください。



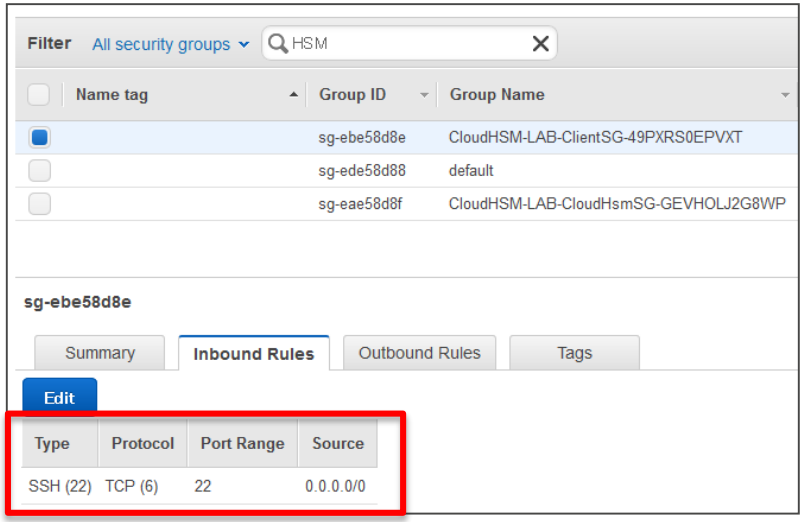
CloudFormationによるインフラ構築

- CloudFormationで構築する環境



Control Instanceへのアクセス

- Control Instanceに付与されている Security Groupの変更
- 特定拠点からのSSHの許可



- CloudHSMアクセス用SSH Keyの作成

```
[ec2-user@ip-172-30-0-241 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ec2-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ec2-user/.ssh/id_rsa.
Your public key has been saved in /home/ec2-user/.ssh/id_rsa.pub.
The key fingerprint is:
af:b6:33:36:35:cb:84:24:45:66:5b:51:cf:c6:f3:23 ec2-user@ip-172-30-0-241
The key's randomart image is:
+--[ RSA 2048]----+
|      .+ oo.     |
|      o.o  +     |
|      ..     *   |
|     . .    . o  |
|      oS.   E ..|
|       ..+   . .|
|        +.o      |
|       *.o       |
|      oo=        |
+-----------------+
[ec2-user@ip-172-30-0-241 ~]$ cd .ssh
[ec2-user@ip-172-30-0-241 .ssh]$ ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts
```

CloudHSM CLIの導入

- ツールの確認と導入を行う
  - Python2.7
  - Easy_install tool
  - CloudHSM CLI Tool

```
[ec2-user@ip-10-0-0-86 .ssh]$ python2.7 -V
Python 2.7.9
[ec2-user@ip-10-0-0-86 .ssh]$ easy_install-2.7 --version
setuptools 12.2
[ec2-user@ip-10-0-0-86 .ssh]$ rpm -qa |grep cloudhsm
[ec2-user@ip-10-0-0-86 .ssh]$ sudo yum install aws-cloudhsm-cli
Loaded plugins: priorities, update-motd, upgrade-helper
amzn-main/latest                                          | 2.1 kB     00:00
amzn-updates/latest                                        | 2.3 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package aws-cloudhsm-cli.noarch 0:3.0.0-1.0.amzn1 will be installed
…….
…
Complete!
[ec2-user@ip-10-0-0-86 .ssh]$
```

CloudHSM CLIの設定

- CloudHSM CLIの設定
  - AWSの認証の設定
    - CloudHSMを操作するためのIAMの認証情報設定（Access Key, Secret Access Key）
    - Cloudhsm CLIを使用する際ーconf_fileとして指定可能

```
[Credentials]
aws_access_key_id = access_key_id
aws_secret_access_key = secret_access_key
aws_region= ap-northeast-1
So_password = XXXXXXXXXX
```

  - SSHコネクションの設定
    - ~/.ssh/configで以下を指定。（ひな形は/etc/ssh/ssh_configから）
    - id_rsaは前のステップでopensslで作成したもの（openssslの場合）

```
Host CloudHSM’s IP Address
User manager
IdentityFile /home/ec2-user/.ssh/id_rsa
```

CloudHSM のプロビジョニング

- CloudHSM のプロビジョニング

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm create-hsm --conf_file ./.cli/cloudhsmcli.conf --subnet-id subnet-6742fxxx --ssh-public-key-file ./.ssh/id_rsa.pub --iam-role-arn
arn:aws:iam::26883621xxxx:role/CloudHSM-LAB-CloudHsmRole-T5SM2ECQO71A --syslog-ip 10.0.0.86

################################################################################################################
                        CloudHSM CLI Tools WARNING
----------------------------------------------------------------------------------------------
Continuing with this command will result in a one-time charge of $5,000 to your AWS account!
If you want to try the CloudHSM service for free, you can request a two week trial by selecting
"Request a free trial" on the following form: https://aws.amazon.com/contact-us/cloudhsm-request/
----------------------------------------------------------------------------------------------
Type 5000 to proceed, anything else to cancel:5000

If you accidentally provisioned an HSM and want to request a refund, please delete the instance
using the 'delete-hsm' command, and then select "Request a refund for an accidental order"
on the following form: https://aws.amazon.com/contact-us/cloudhsm-request/

{
   "HsmArn": "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hsm-9ff64750",
   "RequestId": "55f10d79-2c68-11e5-b332-09794632767c"
}
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm list-hsms --conf_file ./.cli/cloudhsmcli.conf
{
   "HsmList": [
      "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hsm-9ff64750"
   ],
   "RequestId": "705de272-2c68-11e5-b332-09794632767c"
}
```

可用性のためにPrivate Subnetに一つずつ計2台プロビジョンしてください。

CloudHSM のプロビジョニング

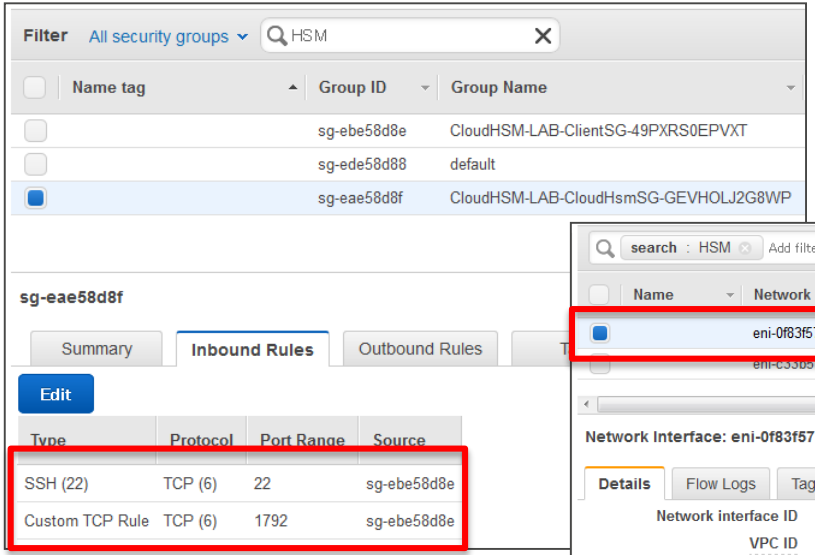
- CloudHSM の状態確認

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm describe-hsm --conf_file ./.cli/cloudhsmcli.conf --hsm-arn arn:aws:cloudhsm:ap-northeast-
1:26883621xxxx:hsm-9ff64750
{
   "EniId": "eni-0f83fxxx",
   "EniIp": "10.0.201.8",
   "HsmArn": "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hsm-9ff64750",
   "IamRoleArn": "arn:aws:iam::26883621xxxx:role/CloudHSM-LAB-CloudHsmRole-T5SM2ECQO71A",
   "RequestId": "0857110b-2c69-11e5-bd87-67c715b7ed9e",
   "SerialNumber": "477768",
   "SoftwareVersion": "5.1.0-25",
   "SshPublicKey": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDrRJKc0UZMNP8FlTp812qLB3vYYLJgNx/skLvKnaTTYjskx7xKLWe1mhCkwAdJLxSRSBMX/0b6F
7QB5UZKVwki5Pbi82hbUfRfkdqDSRncRvgSy1aZNA3b+eKnLvxrJxQk6AbcE5YT2Sfnij49OrdECAjVWc0cRUiBKB89nOrbW/w0+71xfsQnF
HnIswXVzBG51sDqs+zLkTfHk0CZXldf4IYh+ynKDsqULMwG44MohWEsaN15mbc5P1PAN/fWmUFJFTXHjHQMHhd1+PSjkiFqJkLecoNzT/f
d/FMogec36Jqh79ZeqHav6pYQgPpXXXXXXXXXXXXXXXXXXD ec2-user@ip-172-30-0-241",
   "Status": "PENDING",
   "SubnetId": "subnet-6742fxxx",
   "SubscriptionStartDate": "2015-07-17T09:43:56.396Z",
   "SubscriptionType": "PRODUCTION",
   "VendorName": "SafeNet Inc."
}
```

StatusがPENDING -> RUNNINGになるのを待ちます
(検証環境では約10分)

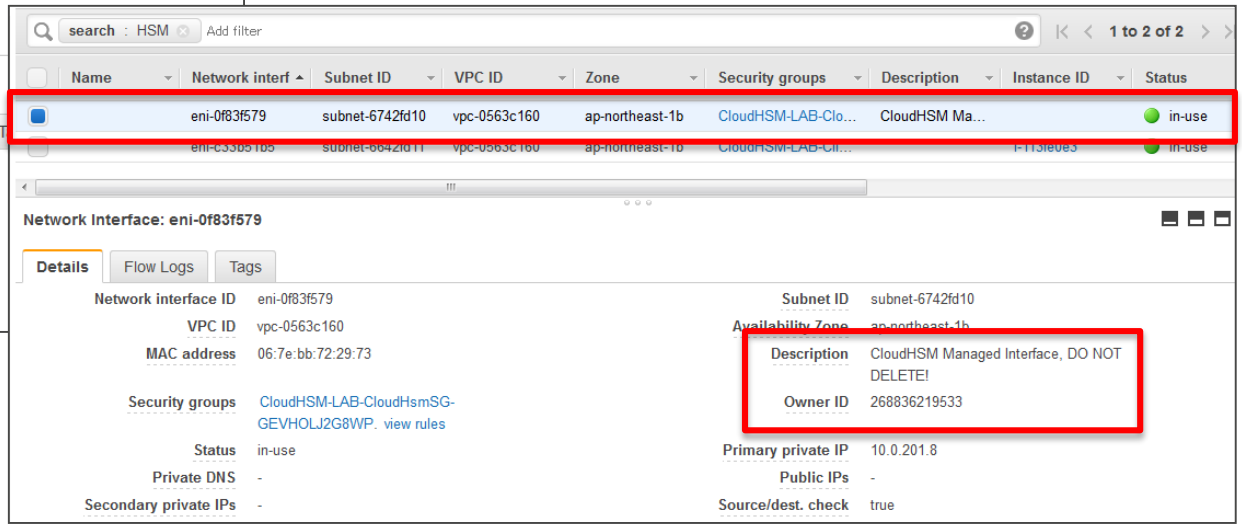
CloudHSM へのアクセス許可設定

- CloudHSM へのアクセス許可



- Cloud HSM用に作成されたSecurity Groupを確認

- Descriptionに“CloudHSM Managed Interface, DO NOT DELETE!” と記載されたENIを探し、予め確認しているSecurity Groupを付与。



CloudHSM の初期化

- CloudHSM の初期化

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm initialize-hsm --conf_file ./.cli/cloudhsmcli.conf --hsm-arn
arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hsm-9ff64750 --label adsjhsm1 --cloning-domain domainxxx
--so-password XXXXXXXXX
{
   "Status": "Initialization of the HSM successful"
}
[ec2-user@ip-10-0-0-86 ~]$
```

HAを組んだCloudHSM間で構成を複製する場合には同じcloning domainである必要があります。

HSM Clientの設定

- Luna SA Client toolsのインストール（Linuxの場合）
  - パッケージのダウンロード
  https://s3.amazonaws.com/cloudhsm-software/610-012382-005_RevB.tar
  - TARを展開してinstall.shの実行。Luna SAのパッケージを導入。
  - /usr/safenet/lunaclientにインストールされる。

```
[ec2-user@ip-172-30-2-155 ~]$ wget  https://s3.amazonaws.com/cloudhsm-software/610-012382-005_RevB.tar
[ec2-user@ip-172-30-2-155 ~]$ tar -xvf 610-012382-005_RevB.tar
[ec2-user@ip-172-30-2-155 ~]$ cd 610-012382-005_RevB/linux/64
[ec2-user@ip-172-30-2-155 64]$ sudo ./install.sh
```

- CloudFormationで作成したControl InstanceのようにCloudHSM Client AMIを利用している場合にはLuna SA Client toolsは既に導入済みとなっています。

HSM Clientの設定

- Luna SA Client tools関係のファイルの所有者とパーミッションの変更
  - /etc/Chrystoki.conf
  - /usr/safenet/lunaclient

```
[ec2-user@ip-10-0-0-86 ~]$ sudo /bin/bash
[root@ip-10-0-0-86 ec2-user]# ls -l /etc/Chrystoki.conf
-r-xr--r-- 1 root root 755 May 26 21:59 /etc/Chrystoki.conf
[root@ip-10-0-0-86 ec2-user]# chown ec2-user /etc/Chrystoki.conf
[root@ip-10-0-0-86 ec2-user]# chmod +w /etc/Chrystoki.conf
[root@ip-10-0-0-86 ec2-user]# cd /usr/safenet
[root@ip-10-0-0-86 safenet]# ls -l
total 4
drwxr-xr-x 8 root root 4096 May 26 21:59 lunaclient
[root@ip-10-0-0-86 safenet]# chown ec2-user -R lunaclient/
```

HSM Clientの設定

- HSM Clientに必要なクライアント証明書と秘密鍵の作成
  - Base64-encoded X.509 v3 PEMの形式

- LunaSA Command（vtl）を利用して作成する場合の例

```
[ec2-user@ip-10-0-0-86 .vtl]$ sudo /usr/safenet/lunaclient/bin/vtl  createCert -n hsm_client1
Private Key created and written to: /usr/safenet/lunaclient/cert/client/hsm_client1Key.pem
Certificate created and written to: /usr/safenet/lunaclient/cert/client/hsm_client1.pem
[ec2-user@ip-10-0-0-86 .vtl]$ cd /usr/safenet/lunaclient/cert/client
[ec2-user@ip-10-0-0-86 client]$ ls -l
total 8
-rw-r--r-- 1 root root 1743 Jul 17 09:29 hsm_client1Key.pem
-rw-r--r-- 1 root root 1164 Jul 17 09:29 hsm_client1.pem
```

Network Trust Linkの作成

- CloudHSMとHSM Clientとで、証明書のコピー
  - CloudHSMからHSM Clientにコピーしてvtlコマンドで登録

```
[ec2-user@ip-10-0-0-86 1]$ scp 10.0.201.8:server.pem .
server.pem                                    100% 1172     1.1KB/s   00:00

[ec2-user@ip-10-0-0-86 1]$ sudo /usr/safenet/lunaclient/bin/vtl addServer -n 10.0.201.8 -c server.pem
New server 10.0.201.8 successfully added to server list.
```

  - HSM ClientからCloudHSMにコピーして登録

```
[ec2-user@ip-10-0-0-86 1]$ scp /usr/safenet/lunaclient/cert/client/hsm_client1.pem 10.0.201.8:
hsm_client1.pem                               100% 1164     1.1KB/s   00:00

[ec2-user@ip-10-0-0-86 1]$ ssh 10.0.201.8
Last login: Wed Jul 22 01:59:51 2015 from 192.168.0.223
Luna SA 5.3.5-1 Command Line Shell - Copyright (c) 2001-2014 SafeNet, Inc. All rights reserved.

[hsm-7-2-1-2] lunash:>client register -client hsm_client1 -hostname hsm_client1
'client register' successful.
```

Network Trust Linkの作成

- パーティションをまだ作成していない場合その作成

```
[hsm-7-2-1-2] lunash:>hsm login
  Please enter the HSM Administrators' password:
  > ************
'hsm login' successful.
Command Result : 0 (Success)

[hsm-7-2-1-2] lunash:>partition create -partition CloudHSM-LAB
Please ensure that you have purchased licenses for at least this number of partitions: 1
If you are sure to continue then type 'proceed', otherwise type 'quit'
> proceed
Proceeding...
  Please enter a password for the partition:
  > ************
  Please re-enter password to confirm:
  > ************
Please enter the cloning domain to use when creating this
partition (press <enter> to use the default domain):
> domainxxx
'partition create' successful.
```

Network Trust Linkの作成

- パーティションに対するClientのアサイン

```
[hsm-7-2-1-2] lunash:>client assignPartition -client hsm_client1 -partition CloudHSM-LAB
'client assignPartition' successful.
Command Result : 0 (Success)

[hsm-7-2-1-2] lunash:>client show -client hsm_client1

ClientID:      hsm_client1
Hostname:      hsm_client1
HTL Required: no
OTT Expiry:    n/a
Partitions:    "CloudHSM-LAB"
```

Network Trust Linkの作成を複数HSMがある場合はそれぞれ行います

```
[ec2-user@ip-10-0-0-86 1]$ /usr/safenet/lunaclient/bin/vtl verify
The following Luna SA Slots/Partitions were found:

Slot    Serial #        Label
====    ========        =====
 1      477768014       CloudHSM-LAB
```

HAPGの構成

- HAPG (high availability partition group)の作成

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm create-hapg --conf_file ./.cli/cloudhsmcli.conf --group-label HAPG1
{
   "HapgArn": "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hapg-142eb13d",
   "RequestId": "febf6f03-3025-11e5-bd88-5162d0aaf0bc"
}
```

- HSMをHAPGに追加（複数台ある場合は別個に追加）

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm add-hsm-to-hapg --conf_file ./.cli/cloudhsmcli.conf --hsm-arn
arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hsm-9ff64750 --hapg-arn arn:aws:cloudhsm:ap-
northeast-1:26883621xxxx:hapg-142eb13d --cloning-domain domainxxx --partition-password XXXXXXXX --
so-password XXXXXXXX
{
   "Status": "Addition of HSM arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hsm-9ff64750 to HAPG
arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hapg-142eb13d successful"
}
```

高可用性設定

- HAPG (high availability partition group)の確認

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm list-hapgs --conf_file ./.cli/cloudhsmcli.conf  {
    "HapgList": [
        "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hapg-142eb13d"
    ],
    "RequestId": "e6fc8f65-3026-11e5-bd88-5162d0aaf0bc"
}
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm describe-hapg --conf_file ./.cli/cloudhsmcli.conf --hapg-arn
arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hapg-142eb13d
{
    "HapgArn": "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hapg-142eb13d",
    "HapgSerial": "0338604349",
    "HsmsLastActionFailed": [],
    "HsmsPendingDeletion": [],
    "HsmsPendingRegistration": [],
    "Label": "HAPG1",
    "LastModifiedTimestamp": "2015-07-22T04:02:44.599Z",
    "PartitionSerialList": [
        "477768018"
    ],
    "RequestId": "079856ce-3027-11e5-bd88-5162d0aaf0bc",
    "State": "READY"
```

Clientの登録

- Clientの作成

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm create-client --conf_file ./.cli/cloudhsmcli.conf --certificate-file
/usr/safenet/lunaclient/cert/client/hsm_client1.pem
{
   "ClientArn": "arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:client-e65aa4be",
   "RequestId": "cb2df1f5-302f-11e5-b332-09794632767c"
}
```

- Clientの登録

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm register-client-to-hapg --conf_file ./.cli/cloudhsmcli.conf --client-arn
arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:client-e65aa4be --hapg-arn arn:aws:cloudhsm:ap-
northeast-1:26883621xxxx:hapg-142eb13d
{
   "Status": "Registration of the client arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:client-e65aa4be to
the HA partition group arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:hapg-142eb13d successful"
}
```

Clientの登録

- Client用の構成ファイルの取得

```
[ec2-user@ip-10-0-0-86 ~]$ cloudhsm get-client-configuration --conf_file ./.cli/cloudhsmcli.conf --client-arn
arn:aws:cloudhsm:ap-northeast-1:26883621xxxx:client-e65aa4be --hapg-arn arn:aws:cloudhsm:ap-
northeast-1:26883621xxxx:hapg-142eb13d --cert-directory /usr/safenet/lunaclient/cert/server/ --config-
directory /etc/
The configuration file has been copied to /etc/
The server certificate has been copied to /usr/safenet/lunaclient/cert/server/
```

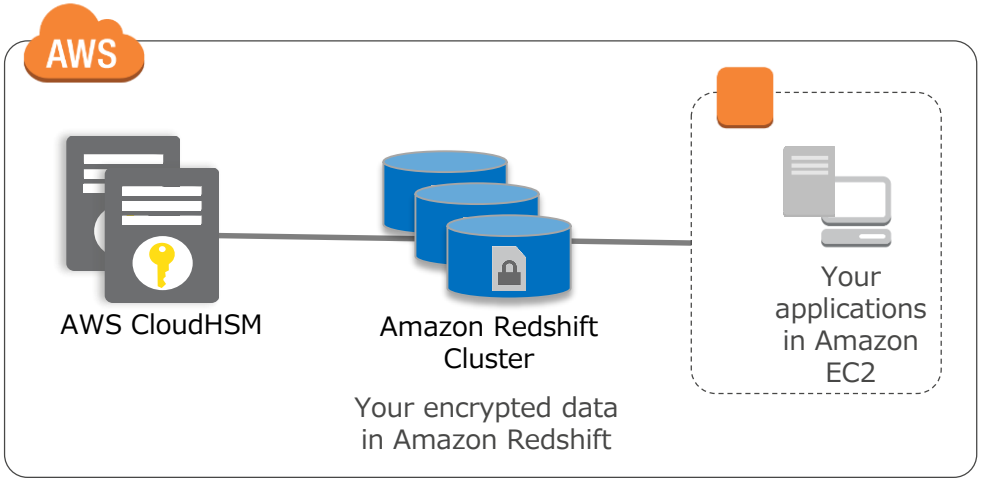
Clientの登録

- 設定の確認

```
[ec2-user@ip-10-0-0-86 ~]$ sudo /usr/safenet/lunaclient/bin/vtl  haAdmin show
================= HA Global Configuration Settings ================
                  HA Proxy:  disabled
             HA Auto Recovery:  enabled
   Maximum Auto Recovery Retry:  Infinite
   Auto Recovery Poll Interval:  60 seconds
                 HA Logging:  disabled
          Only Show HA Slots:  yes
================= HA Group and Member Information =================
            HA Group Label:  HAPG1
           HA Group Number:  2800879602
           HA Group Slot #:  1
           Synchronization:  enabled
             Group Members:  477768018, 477795018
           Standby members:  <none>
Slot #    Member S/N                Member Label    Status
======    ==========                ============    ======
   -    477768018          hapg-142eb13d_477768    alive
   -    477795018          hapg-142eb13d_477795    alive
```

Redshiftでの利用方法

- クラスタキーの保管にCloudHSMを利用
  - RedshiftはHSMにクラスタキーの生成をリクエスト（HSMはクラスタキーを保管）
  - Redshiftはクラスタキーを使ってデータベースキーを暗号化
  - HSMはクラスタキーを利用して暗号化されたデータベースキーを復号。セキュアチャネルを通してRedshiftクラスタに渡す
  - クライアント側にソフトウェアは不要

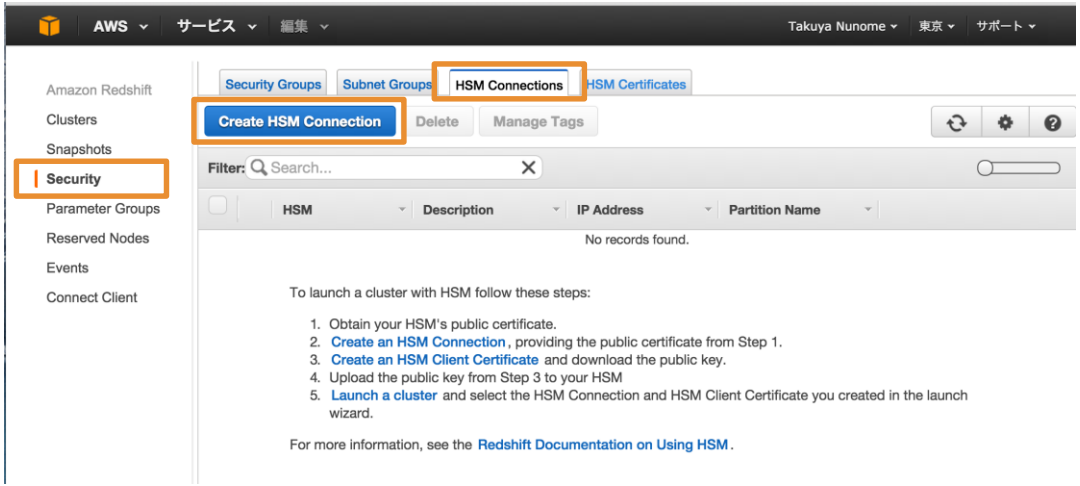


Redshiftでの利用方法

- 利用ステップ
  1. HSM接続の作成
     CloudHSMとの接続に必要な各種情報を定義
  2. HSMクライアント証明書の作成と登録
     クラスタ用のクライアント証明書を生成し、CloudHSMに登録
  3. クラスタの作成
     作成したHSM接続・クライアント証明書を利用してRedshiftクラスタインスタンスを作成

Redshiftでの利用方法
1.HSM接続の作成

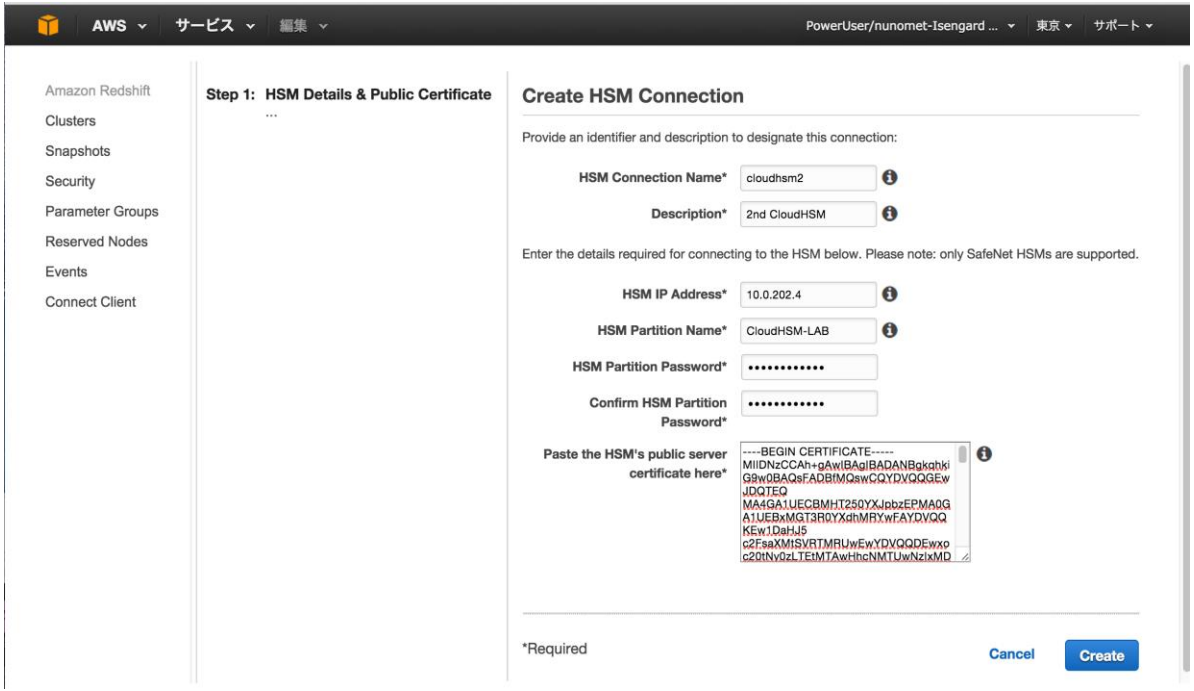
- Redshiftコンソールから、「Security」→「HSM Connections」→「Create HSM Connections」を選択



Redshiftでの利用方法
1.HSM接続の作成

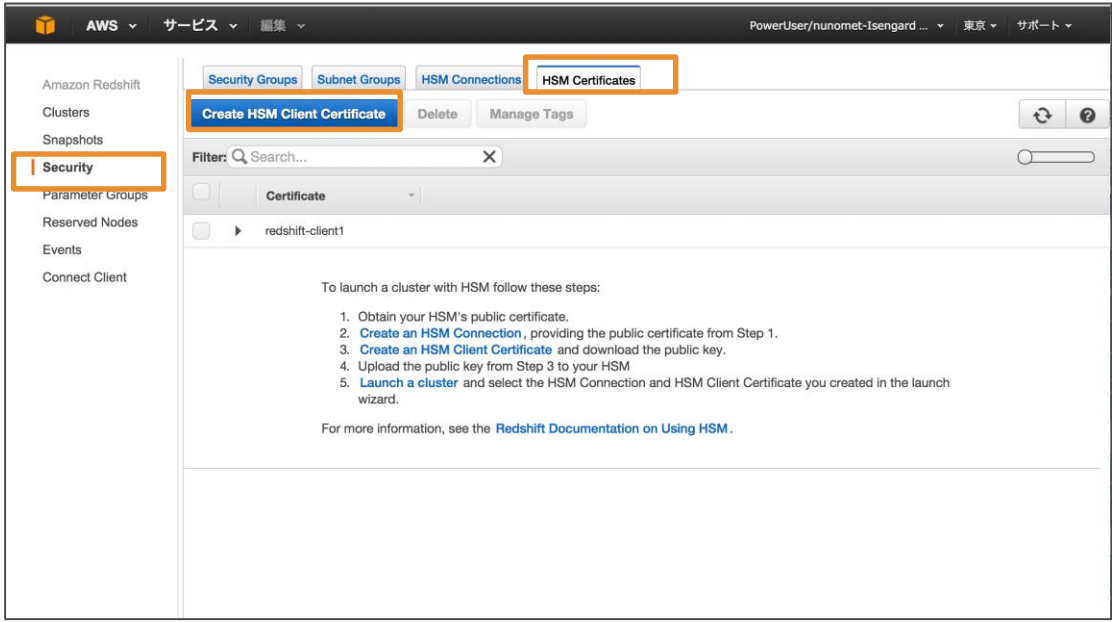
- HSM側の情報を入力
  - 接続名（任意）
  - Description（任意）
  - HSMのIPアドレス※
  - HSMのパーティション名
  - パーティションのパスワード
  - HSMのサーバ証明書
    - HSMクライアントにて取得

※RedshiftクラスタとHSMはNTLSで通信可能となるよう事前にサブネットやSecurity Groupの
設定を実施しておく必要があります。



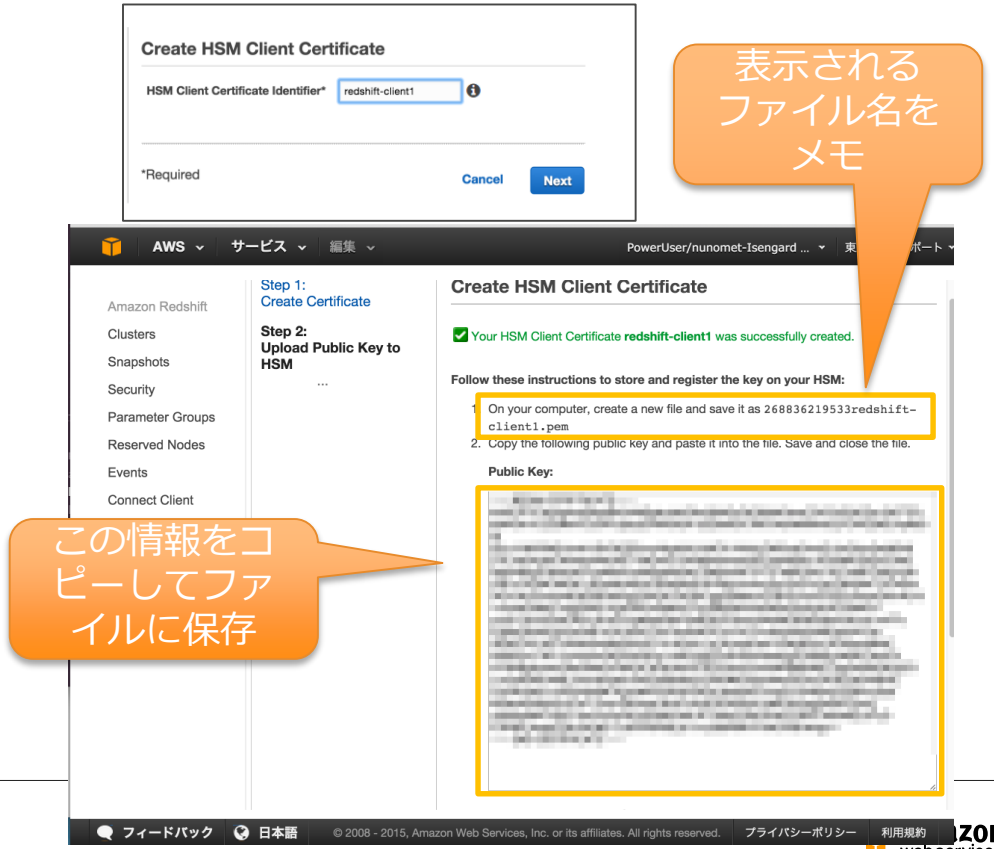
Redshiftでの利用方法
2.クライアント証明書の作成と登録

- Redshiftコンソールから、「Security」→「HSM Certificates」→「Create HSM Certificate」を選択



Redshiftでの利用方法
2.クライアント証明書の作成と登録

- HSM Client certificate identifier(任意)を入力し、「Next」をクリックすると、クライアント証明書が作成される
- 表示された証明書をコピー&ペーストで<表示された名前>.pemに保存



Redshiftでの利用方法
2.クライアント証明書の作成と登録

- コントロールクライアントからscpコマンドでPEMファイルをHSMに転送

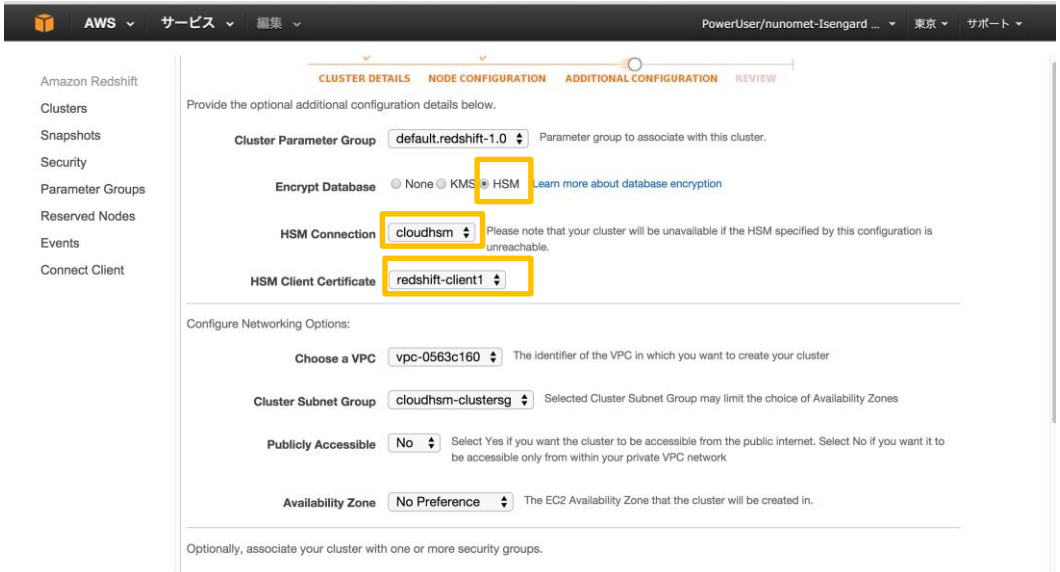
```
[ec2-user@ip-10-0-0-86]$ scp 26836219533redshift_client1.pem 10.0.201.8:
26836219533redshift_client1.pem                    100% 1164     1.1KB/s   00:00
```

- CloudHSMにログインし、PEMファイルをHSMに登録

```
[ec2-user@ip-10-0-0-86 ~]$ ssh 10.0.201.8
[hsm-7-2-1-2] lunash:>client register -client redshift-client1 -hostname 268836219533redshift-client1

'client register' successful.

[hsm-7-2-1-2] lunash:>client list

registered client 1: hsm_client1
registered client 2: redshift-client1

[hsm-7-2-1-2] lunash:>client assignPartition -client redshift-client1 -partition CloudHSM-LAB

'client assignPartition' successful.
```

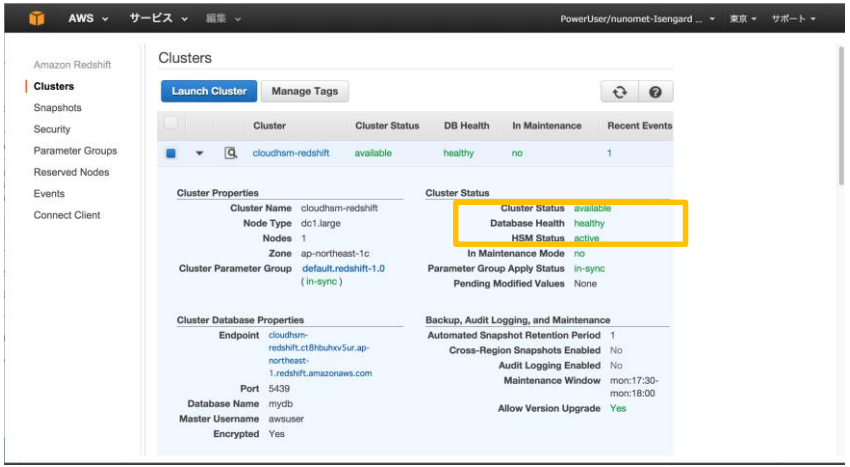
Redshiftでの利用方法
3.クラスタの作成

- クラスタ作成時に以下を指定
  - Encrypt Database
    「HSM」を指定
  - HSM Connection
    作成したHSM接続を指定
  - HSM Client Certificate
    作成したCertificateを指定



Redshiftでの利用方法
3.クラスタの作成

- クラスタ作成が正常に完了すると、Cluster Statusが以下の状態になる
  - Cluster Status: available
  - Database Health: healthy
  - HSM Status: Active



- CloudHSMから、Redshift用のマスターキーの状態が確認可能

```
[hsm-7-2-1-2] lunash:>partition showContents -partition CloudHSM-LAB
Please enter the user password for the partition:  > ************
Partition Name:  CloudHSM-LAB
Partition SN:    477768014
Storage (Bytes): Total=102701, Used=168, Free=102533
Number objects:  1
Object Label:  cluster35429ts1437552287861-1
Object Type:   Symmetric Key
```

CloudHSMの停止

- CFテンプレートで構築されたコントロールインスタンスにSSHでアクセス
  - SSHでCloudHSMにアクセス
  - “Zeroize”の実施。HSM Administratorとしてのログイン失敗を3度繰り返す

  lunash:> hsm login
  - ログの削除

  lunash:> syslog rotate

  lunash:> syslog cleanup
  - CloudHSM CLIのdelete-hsmかAPIのDeleteHsmによる削除

- 不明な点があればサポートにコンタクトを

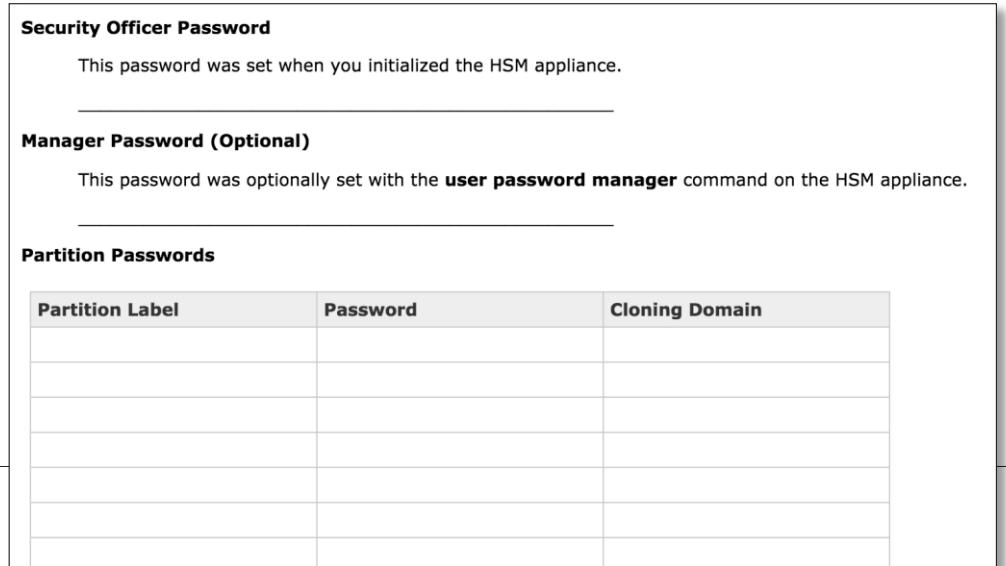
- 不払いのような状況のためにAWSはお客様のCloudHSMをTerminateする権利を有しています。

CloudHSMの推奨事項

- 2つ以上のAZを用いて、複数のCloudHSMにより冗長構成をとること。シングル構成でCloudHSMに障害が起きた場合、鍵は完全に失われます。
- 暗号鍵が完全に必要でなくなった、もしくはバックアップを取った場合を除き、初期化は行わないでください。
- ソフトウェアパッチやアップデートを自分で行わないでください。必ずAWSサポートにコンタクトをしてください。
- CloudHSMのネットワーク構成を変更することは避けてください
- Syslog転送が可能ですので必ず取得するようにしてください
- SnmpやNTPの設定を変更することは避けてください。

パスワードに関する推奨事項

- CloudHSMのso_password (Security Officerパスワード) はパスワードワークシートに記述し厳重に保管をしてください。
- またこのワークシートのコピーをセキュアなオフサイトにも厳重に保管することを推奨します。
- CloudHSMの管理者パスワードは変更しないでください。これはAWSがサービスをデリバリーする際にも利用されます。
- CloudHSMへのSSHアクセスにはSSH Keyを利用してください。



Security Officer Password

This password was set when you initialized the HSM appliance.

_____

Manager Password (Optional)

This password was optionally set with the **user password manager** command on the HSM appliance.

_____

Partition Passwords

Partition Label	Password	Cloning Domain

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

価格

- CloudHSM インスタンスを 1 つ立ち上げるごとに、初期費用料金
- インスタンス終了までの間、1 時間ごとに時間料金
- CloudHSM サービスを無料でお試しになる場合は、2 週間のトライアルをリクエスト可能。応募資格については、無料トライアルページを確認
  http://aws.amazon.com/jp/cloudhsm/free-trial/
- CloudHSMにはStopがありません。停止するにはTerminateが必要で、再度利用する際には前払い金が発生します。

前払い金	時間単価	月平均のランニング
$5,000	$2.82/h	$2,059

CloudHSMの制限

1アカウント、1リージョン当たり以下の制限があります。

Limits	Thresholds
HSM アプライアンス	3
High-availability partition groups	20
クライアント	800

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

KMS アップデート

- Amazon Elastic MapReduceにおけるクライアントサイド暗号化のサポート

  https://aws.amazon.com/releasenotes/AWS-KMS/149877887892099 2

- Amazon RDS for SQL Server および Oracleのサポート

  https://forums.aws.amazon.com/ann.jspa?annID=2977

- AWS GovCloud (US) Regionでの利用開始

※2015年2月以降のアップデート

KMSがサポートするAWSサービス

カテゴリ	サービス	対応機能
データベース	Amazon Redshift	クラスターキー管理
	Amazon RDS (MySQL, PostgreSQL, **SQL Server, Oracle**) New !	データベースストレージの暗号化
ストレージ・コンテンツ配信	Amazon Simple Storage Service	サーバサイド暗号化(SSE-KMS)
		S3 Encryption Clientを利用したクライアントサイド暗号化
	Amazon Elastic Block Store(EBS)	ボリューム暗号化
アプリケーションサービス	Elastic Transcoder	トランスコードデータ暗号化
	WorkMail	保存データ(メール、コンタクト、添付ファイル、メタデータ)の暗号化
分析	**Amazon Elastic MapReduce** New !	EMRFSのクライアントサイド暗号化

RDSのKMS対応DBエンジンの追加

- KMSで鍵の管理が可能
  - ストレージの暗号化
  - AES-256
- 対応DBエンジンにMySQL、PostgreSQLに加えて、Oracle、SQLServerが追加
- 対応インスタンスタイプ
  - db.m3.* db.r3.*
  - db.cr1.8xlarge(旧世代)
- RDS for Oracleでは、CloudHSMによるTDEとの併用も可能

Amazon Elastic MapReduceでのクライアントサイド暗号化サポート

- EMRFS(S3)のクライアントサイド暗号化でKMSをサポート
- クラスター作成時に暗号化プロバイダを指定
  - マネージメントコンソール、CLIどちらかで指定
- 2つの暗号化プロバイダをサポート
  - AWS提供のKMSプロバイダ
  - カスタム Java プロバイダ
- カスタムJavaプロバイダの詳細は以下を参照

https://docs.aws.amazon.com/ja_jp/ElasticMapReduce/latest/DeveloperGuide/emr-plan-cse-custom.html

CloudHSMとKMSの使い分け

- 規制や法令の対応により、認定を受けた鍵管理モジュールが必要
- 現在SafeNetのHSMをオンプレミスで利用している
- 公開鍵暗号化も行いたい
- 暗号化処理をオフロードしたい
- 秒間100を超えるような暗号化リクエストがある
- 隔離された専用環境で厳格に鍵管理したい

CloudHSM

- 共通鍵暗号のみ利用
- 鍵管理は自分で行いたい
- 手軽かつ安全に暗号化処理を利用したい
- より低コストに鍵管理の仕組みを利用したい
- AWSサービスで簡単に利用したい
- 保管されるデータの暗号化がメイン
- CloudTrailによる監査を行いたい

KMS

アジェンダ

- AWS CloudHSMの概要
- CloudHSMのユースケース
- CloudHSMの利用方法
- 料金・制限等
- AWS KMSアップデート
- まとめ

まとめ

- CloudHSMを利用すると業界標準の不正使用防止策が施された HSM アプライアンスで暗号キーを保護/保管することができます。
- ユーザー以外にはキーへのアクセスを許可することができません（アプライアンスを管理/保守するAmazonの管理者もアクセスできません）。
- 安全な鍵管理に対する米国政府標準規格に適合するように設計/検証されたHSM内で暗号鍵を保護することができるようになります。
- アプリケーションのパフォーマンスを低下させることなく、厳密なキー管理要件に準拠することができます。

Webinar資料の配置場所

- AWS クラウドサービス活用資料集
  - http://aws.amazon.com/jp/aws-jp-introduction/

プロダクト別：				
Amazon S3		AWSマイスターシリーズ Re:Generate Amazon Simple Storage Service (S3)	Slideshare	PDF
Amazon Glacier		AWSマイスターシリーズ Reloaded Amazon Glacier Amazon Glacierのご紹介 機能編	Slideshare（Reloaded） Slideshare（機能編）	PDF（Reloaded） PDF（機能編）
Amazon Route 53		AWSマイスターシリーズ Re:Generate	Slideshare	PDF

公式Twitter/Facebook
AWSの最新情報をお届けします

@awscloud_jp

もしくは
http://on.fb.me/1vR8yWm

最新技術情報、イベント情報、お役立ち情報、お得なキャンペーン情報などを
日々更新しています！

AWS運用コミュニティ

～クラウドによる、クラウドのための、クラウド運用管理～

AWS上に構築されたシステムの
運用管理のベストプラクティスを集約！

@opsjaws

http://aws.typepad.com/aws_partner_sa/2015/06/aws-ops.html

ご参加ありがとうございました。