



**Administració
Oberta de
Catalunya**

PSIS: CloudHSM


Data: 24/01/2025



**Generalitat
de Catalunya**

Localret

Control documental

Estat formal	
Elaborat per	
Aprovat per	Áurea Alcaide Izquierdo
Data de creació	24/01/2025
Nivell accés informació	Pública
Títol	PSIS: CloudHSM
Fitxer	PSIS-CloudHSM.docx
Control de còpies	Només les còpies disponibles a la Seu electrònica del Consorci AOC garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.
Drets d'autor	<p>Aquesta obra està subjecta a una llicència Reconeixement - No comercial- Sense obres derivades 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p> 

Control de versions

Data:	24/01/2025
Descripció:	Creació del document
Data:	
Descripció:	

Índex

PSIS: CloudHSM.....	1
Control documental	2
Control de versions	2
Índex	3
1. Creació i eliminació del CloudHSM clúster	4
1.1. Entorn de DEV	4
1.1.1. Step Functions	4
1.1.2. AWS EventBridge	5
1.2. Entorn de PRO.....	6
2. Paràmetres i Secrets a AWS	6
2.1. Parameter Store	6
2.2. Secrets Manager	7
3. Gestió de claus amb el CloudHSM CLI	7
3.1. Llistat de claus	8
3.2. Esborrar una clau.....	13
4. CloudHSM JCE Provider	13
4.1. Descàrrega.....	14
4.1.1. Última versió	14
4.1.2. Versió concreta	14
4.2. Instal·lació per compilar el codi	15
4.2.1. Local	15
4.2.2. Jenkins.....	15
4.3. Procediment d'actualització.....	16

1. Creació i eliminació del CloudHSM clúster

Els entorns de DEV i PRE no fan servir HSM. Tanmateix, per fer proves, podem aixecar un CloudHSM clúster a l'entorn de DEV, i configurar PSIS i la consola per a que facin servir el CloudHSM clúster. El clúster està accessible tant des de tots dos entorns.

1.1. Entorn de DEV

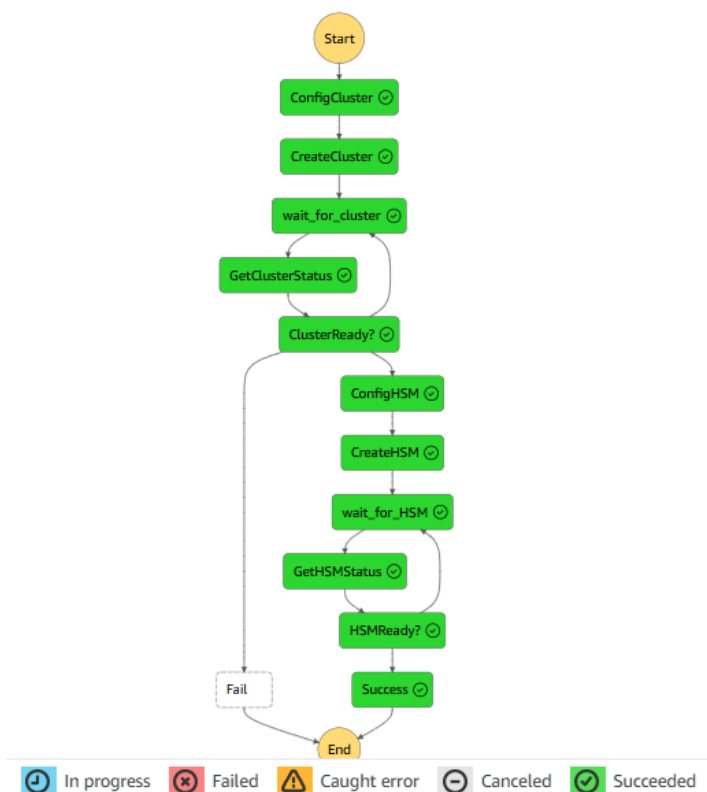
A l'entorn de DEV disposem d'un parell de Step Functions (o State Machines) que ens permeten tant aixecar com eliminar un CloudHSM clúster.

Creació i manteniment de les Step Functions: Claranet

1.1.1. Step Functions

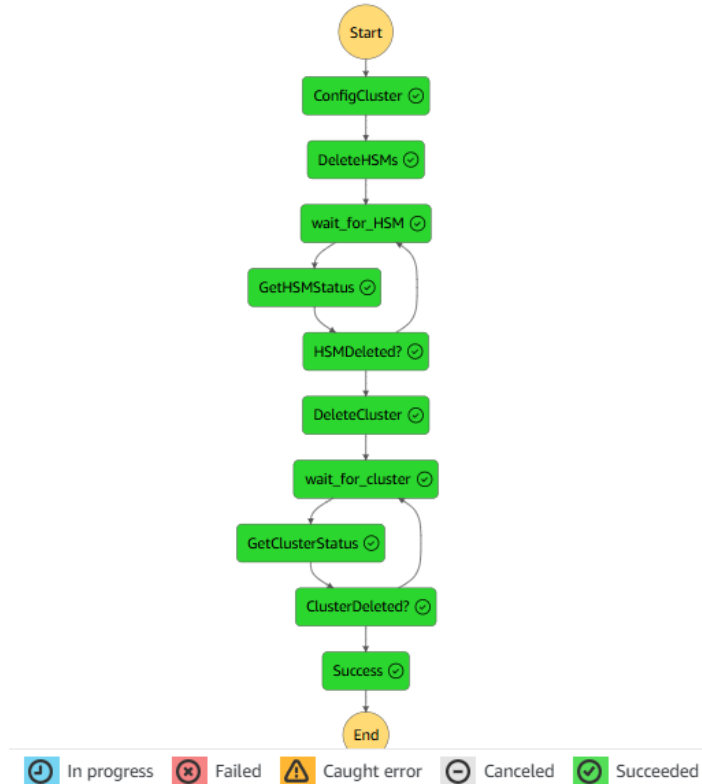
- **sft-dev-psis-createcluster**

Crea el CloudHSM clúster, amb 2 HSMs.



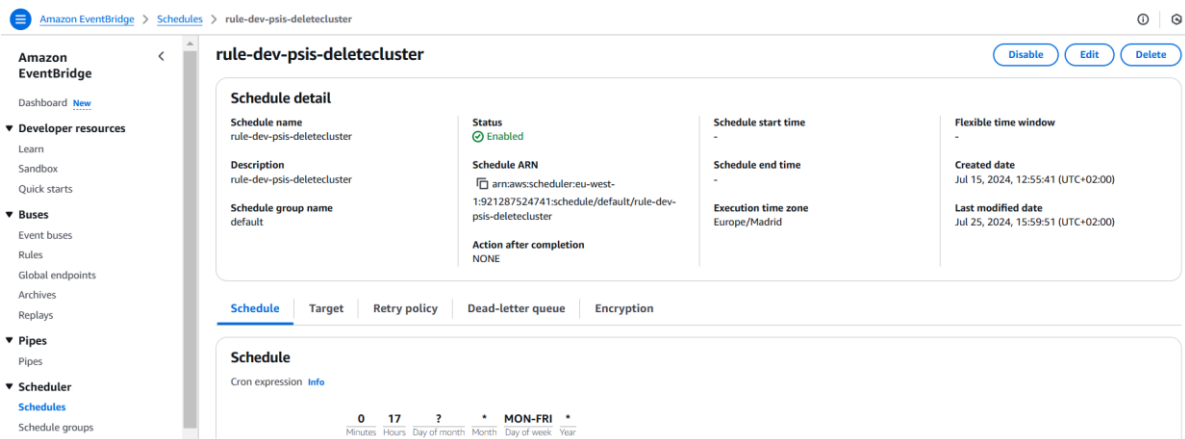
- **sft-dev-psis-deletecluster**

Crea un backup i elimina el CloudHSM clúster.



1.1.2. AWS EventBridge

Per evitar costos innecessaris, tenim programat un scheduler que executa cada dia, de dilluns a divendres, a les 17h, la Step Function anterior d'esborrar el CloudHSM clúster:



Amazon EventBridge > Schedules > rule-dev-psis-deletecluster

Schedule detail

Schedule name rule-dev-psis-deletecluster	Status Enabled	Schedule start time -	Flexible time window -
Description rule-dev-psis-deletecluster	Schedule ARN arn:aws:scheduler:eu-west-1:921287524741:schedule/default/rule-dev-psis-deletecluster	Schedule end time -	Created date Jul 15, 2024, 12:55:41 (UTC+02:00)
Schedule group name default	Action after completion NONE	Execution time zone Europe/Madrid	Last modified date Jul 25, 2024, 15:59:51 (UTC+02:00)

Schedule

Cron expression: `0 17 ? * MON-FRI *`

Minutes: 0, Hours: 17, Day of month: ?, Month: *, Day of week: MON-FRI, Year: *

The screenshot shows the Amazon EventBridge console. On the left is a navigation menu with options like Dashboard, Developer resources, Buses, Pipes, Scheduler, and Integration. The main area displays the details for a schedule named 'rule-dev-psis-deletecluster'. The 'Schedule detail' section shows the schedule name, description, group name, status (Enabled), ARN, start/end times, execution zone, and creation/modification dates. The 'Target' section shows the target name, ARN, service (AWS Step Functions), and API (StartExecution).

1.2. Entorn de PRO

A l'entorn de PRO el CloudHSM clúster no s'elimina, està aixecat les 24 hores, doncs a PSIS PRO es fan servir única i exclusivament claus en HSM. Per tant, no es van crear les Step Functions anteriors per aquest entorn.

Gestionat exclusivament per Claranet.

2. Paràmetres i Secrets a AWS

Passem a descriure els diferents paràmetres que tenim a AWS relacionats amb CloudHSM.

2.1. Parameter Store

Els paràmetres que ens permeten configurar PSIS i la consola de PSIS per fer servir o no CloudHSM són:

Paràmetre	Possibles valors	Descripció
/config/psis/cloudhsm.enabled	true / false	Indicarem "true" quan volguem configurar PSIS per treballar amb les claus en HSM, i "false" per treballar amb claus en base de dades (PostgreSQL).
/config/psis/signatureservice.provider	CloudHSM / BC	Indica el proveïdor criptogràfic. Si cloudhsm.enabled té el valor "true", el proveïdor haurà de ser "CloudHSM". Si està a "false", aleshores és BC (BouncyCastle). Actualment són aquests els 2 proveïdors criptogràfics que PSIS suporta.

Els següents paràmetres són usuaris del CloudHSM, i les IPs del clúster:

Paràmetre	Valor	Descripció
/infra/hsm/psis-pro/admin.user	admin	Usuari administrador del CloudHSM clúster.
/infra/hsm/psis-pro/app.user	psisuser	Usuari criptogràfic de l'aplicació.
/infra/hsm/psis-pro/cluster.ips		IPs separades per comes, dels HSMs del clúster.

2.2. Secrets Manager

Els passwords dels usuaris anteriors es troben al Secrets Manager:

Paràmetre	Descripció
/infra/hsm/psis-pro/admin.pwd	Password de l'usuari administrador del CloudHSM clúster.
/infra/hsm/psis-pro/app.user.pwd	Password de l'usuari criptogràfic de l'aplicació.

Al Secrets Manager també es generen una sèrie de secrets necessaris per la connexió al CloudHSM clúster:

Paràmetre	Descripció
/infra/hsm/psis-pro/cert-init-cluster	<i>Certificate to init cluster. 20 year expiration. Created by init.sh script.</i>
/infra/hsm/psis-pro/customer-ca-key	<i>Customer CA private key. Created by 01_generate_cloudhsm_certs.sh script.</i>
/infra/hsm/psis-pro/customer-ca-cert	<i>Customer CA certificate in base64. 20 year expiration. Created by 01_generate_cloudhsm_certs.sh script.</i>

3. Gestió de claus amb el CloudHSM CLI

El client de CloudHSM el tenim instal·lat a la màquina Bastion de DEV. Per gestionar claus al CloudHSM de forma directa, ho podem fer mitjançant aquest client.

Documentació:

[Key management with CloudHSM CLI](#)

- Accedir a la shell del Bastion:

Per accedir a la shell del Bastion, ho farem des de la consola d'AWS:

Accedir a la instància **EC2 del Bastion**, clicar **“Connect”**, opció **“Session manager”**.

Executar "bash" (si no hi ha problemes amb tecles i demés...).

Configurar el client CloudHSM amb una de les IPs dels HSMs del clúster CloudHSM:

```
sudo /opt/cloudhsm/bin/configure-cli -a 10.140.149.198
```

La IP la podem obtenir consultant les que estan guardades al paràmetre següent del Parameter Store:

```
/infra/hsm/psis-pre/cluster.ips
```

O també directament a la consola d'AWS, al ClusterHSM, on se'ns informa de les adreces ENI IPv4 de cadascun dels HSMs.

- Arrencar el client:

/opt/cloudhsm/bin/cloudhsm-cli interactive

Fer login amb usuari (psisuser) que es trobi al paràmetre:

```
/infra/hsm/psis-pro/app.user
```

El password el tenim al secret:

```
/infra/hsm/psis-dev/appuser.pwd
```

```
aws-cloudhsm > login --username psisuser --role crypto-user
Enter password:
{
  "error_code": 0,
  "data":
  { "username": "psisuser", "role": "crypto-user" }
}
```

Exemple:

```
sudo /opt/cloudhsm/bin/configure-cli -a 10.140.149.14
/opt/cloudhsm/bin/cloudhsm-cli interactive
aws-cloudhsm > login --username psisuser --role crypto-user
```

3.1. Llistat de claus

La comanda per veure les claus que tenim al clúster CloudHSM és:

key list

Cada clau està identificada per atributs. Per exemple:

```
{
  "key-reference": "0x0000000000000007",
  "attributes":
  { "label": "XI+3TbZqigKDYKeZiVRoOF849Kg=" }
}
```

Si volem informació detallada:

key list --verbose

Exemple de sortida:

```
aws-cloudhsm > key list --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x000000000000000008",
        "key-info": {
          "key-owners": [
            {
              "username": "psisuser",
              "key-coverage": "full"
            }
          ],
          "shared-users": [],
          "cluster-coverage": "full"
        },
        "attributes": {
          "key-type": "rsa",
          "label": "20250122011603924ioZvuXjX3+BRy9RsbMQ+xA2MnvU=",
          "id": "0x",
          "check-value": "0x59a6d8",
          "class": "private-key",
          "encrypt": false,
          "decrypt": true,
          "token": true,
          "always-sensitive": false,
          "derive": false,
          "destroyable": true,
          "extractable": true,
          "local": false,
          "modifiable": true,
          "never-extractable": false,
          "private": true,
          "sensitive": true,
          "sign": true,
          "trusted": false,
          "unwrap": true,
          "verify": false,
          "wrap": false,
          "wrap-with-trusted": false,
          "key-length-bytes": 1217,
          "public-exponent": "0x010001",
          "modulus":
            "0xad32613629f9273e743616039649df24ec27e211895634abe76288de907ae480ed26f47
            e7d34f51dfac1035744c609566dc4c08eda9e05f5ae565a10d22c7290e388618ec66e55152
            011e841f855a768477d484f76eb9c4d83e37984e30d8ca2491cfd002b92a2bb70c6b1008c2
            28a3bb888783a4fc260e9afa6646118c9634c350ef653355917d91435c60de8766a9e9b08fa
            6ea4b785982b46b83da167f9664c41a0743b8155a2107dcb88995aaf43486b386a78956f67
```

```

deb2f662db16787dd647f1fcd7c176383bbdd2db5fe4b690be7ad31dd5e416121754bf2f479
6a7c293182e5dd6b54fa83b295f617f7d5fc4b4df072bd4bfd67f495a69665abd08f1",
  "modulus-size-bits": 2048
}
},
{
  "key-reference": "0x00000000000040006",
  "key-info": {
    "key-owners": [
      {
        "username": "psisuser",
        "key-coverage": "full"
      }
    ],
    "shared-users": [],
    "cluster-coverage": "full"
  },
  "attributes": {
    "key-type": "rsa",
    "label": "20250122011617863XI+3TbZqigKDYKeZiVRoOF849Kg=",
    "id": "0x",
    "check-value": "0xfe3156",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": false,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": false,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
    "wrap": false,
    "wrap-with-trusted": false,
    "key-length-bytes": 1219,
    "public-exponent": "0x010001",
    "modulus":
"0xd6d37f00e2b60fea774642710afe48fb3fd7d68158e1689f61a1c11429ccf95203fbeda766
5b6466c2e2d8f19bde9821b613ef04eb00bada8b3b4cc3ac3dfc68c04a79b5fec14b6b5c0dc
9b0a26e855fcabc59b8ff8e69d47bee2a620f0ef26c1659e68419fe69c17dabc3c061a68c0b8b
a53c4893bac3b69e7f008ed2e6af77ccd536ac977b134481f9d479867e6da8bd2b48a6d406
e7cd504824f22ac37556632857ad4b134f789c9212d261bffc3833b5f322f2b45b1e31555582
de98a29e5975ed37372ffb2b7a3cc632a602b0c15325c8c39e4ff132769152662f218143060
9da5a9283e4f9813720598cfc7ccd7828380e884a2d311547fa679b116c481",
    "modulus-size-bits": 2048
  }
}

```

```

    },
    {
      "key-reference": "0x00000000000040007",
      "key-info": {
        "key-owners": [
          {
            "username": "psisuser",
            "key-coverage": "full"
          }
        ],
        "shared-users": [],
        "cluster-coverage": "full"
      },
      "attributes": {
        "key-type": "rsa",
        "label": "20250122011547920EHXmj5i63LR9u9UanvyauZI2TyA=",
        "id": "0x",
        "check-value": "0x653c82",
        "class": "private-key",
        "encrypt": false,
        "decrypt": true,
        "token": true,
        "always-sensitive": false,
        "derive": false,
        "destroyable": true,
        "extractable": true,
        "local": false,
        "modifiable": true,
        "never-extractable": false,
        "private": true,
        "sensitive": true,
        "sign": true,
        "trusted": false,
        "unwrap": true,
        "verify": false,
        "wrap": false,
        "wrap-with-trusted": false,
        "key-length-bytes": 1217,
        "public-exponent": "0x010001",
        "modulus":
"0xb02c97e7c4043ce8a4a527b69deac04075952d07f605f6e778ae9b61d9cacf6baf2ec9b2
a3424ab8c8b77fecf1705541805d0b72b69823a1991719aa7fa211ce12e4a48201d15d5d14
eeca17c1e383aca91950982dfd24fdeef7b0a908de1805631fc73ecbb9804e49912b80d1316
078b961b3d3cdfc05ffcdabc487c4892577ecc7f5fbb53679ac49a4392164a1ade70ae4a2bb30
ca7e54450ad2089466421385e4e8bd63cacb23497c7e8c8f786d40abc3a05d7603690ad94
afa96a1f0ec9222a5b4b1132ad4473cc5d9657e37fe76f74e38a16b118c5f884e85b755e55d
8377b95176a6acd9e184c8970a808432c1d8e618625bc1c315d490b9208b9a2660d",
        "modulus-size-bits": 2048
      }
    },
    {
      "key-reference": "0x00000000000040009",
      "key-info": {

```

```

    "key-owners": [
      {
        "username": "psisuser",
        "key-coverage": "full"
      }
    ],
    "shared-users": [],
    "cluster-coverage": "full"
  },
  "attributes": {
    "key-type": "rsa",
    "label": "20250122011633728cn5/ztcgl3eZg0P9r4BZWTcndlg=",
    "id": "0x",
    "check-value": "0x299ec4",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": false,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": false,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
    "wrap": false,
    "wrap-with-trusted": false,
    "key-length-bytes": 1217,
    "public-exponent": "0x010001",
    "modulus":
"0x9190451d84b371c22212a2be6d696e9b82a8490e45fcc9bc9273c30276acbd61c15b1d6
8cc755455ed5c3bf19c6ea997d187f844c84168ea75a9733c3d36112ac02580ddd3add72d3
d05c1e8634ffe6cae832fd89186fa07e966848af1624a248c4de769114976a4851353a7967f2
c1c31c4af93726dd631182cac60b67aa88f61bd0f34f15f153033bf40cacd814942f0183c53ec
d403377cfc64ba627a034d903522d1aac511627af0e0c95bdc16048c1a13e4474bfdcbb225b
533fd6f579a8665f8d8b0ca672317c08e73fee5c99cfee73d8edfa5681a51e5382d9b3a4d649
a67531812a0f2d8cd2e331ff3d10252ba218d1d66277a1bcb87fc105f8d3ca7",
    "modulus-size-bits": 2048
  }
}
],
"total_key_count": 4,
"returned_key_count": 4
}
}

```

3.2. Esborrar una clau

L'esborrat de claus s'ha de fer una a una.

La comanda per esborrar una clau és:

key delete --filter attr.label="*label*"

On "*label*" és l'atribut "*label*" que podem consultar en extreure el llistat de claus.

Exemple de sortida, si tot ha anat correctament:

```
Keu delete --filter attr.label="20250122011633728cn5/ztcgl3eZg0P9r4BZWTcndlg="
{
  "error_code": 0,
  "data":
  { "message": "Key deleted successfully" }
}
```

IMPORTANT: *En el cas de PSIS hem fet que el label sigui únic per cada clau, afegint la data fins als mil·lisegons al label. Això també ens permet distingir de quina clau es tracta, tenint coneixement de quin dia es va carregar.*

El fet és que no es poden eliminar vàries claus a l'hora. Així evitem tenir claus amb el mateix label.

En cas d'intentar eliminar una clau amb un label que no sigui únic:

```
{
  "error_code": 1,
  "data": "Key selection criteria matched 2 keys. Refine selection criteria to select a single key."
}
```

Per solucionar-ho, canviar per exemple l'atribut label amb la comanda "set-attribute", que sí permet especificar el key-reference:

```
key set-attribute --key-reference 0x00000000000040006 --name "label" --value "l1"
key delete --filter attr.label=l1
```

Documentació de la comanda "set-attribute":

https://docs.aws.amazon.com/cloudhsm/latest/userguide/cloudhsm_cli-key-set-attribute.html

4. CloudHSM JCE Provider

Per poder treballar amb el CloudHSM clúster des de codi java, necessitem el JCE provider per AWS CloudHSM.

A la següent URL tenim informació sobre com instal·lar-ho:

[Install the JCE provider for AWS CloudHSM Client SDK 5](#)

4.1. Descàrrega

Actualment estem fent servir la següent versió de Linux, tant pel core de PSIS com per la consola : **Ubuntu 20.04 LTS**

4.1.1. Última versió

Per a aquesta versió concreta, podem descarregar l'última versió del JCE provider des de :

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Focal/cloudhsm-jce\_latest\_u20.04\_amd64.deb
```

I instal·lar-lo amb la comanda :

```
sudo apt install ./cloudhsm-jce_latest_u20.04_amd64.deb
```

A l'arxiu cloudhsm-jce...._u20.04_amd64.deb, si el descomprimim, trobarem la llibreria que ens interessa: `cloudhsm-jce-version.jar`, on *version* correspondrà a la darrera versió publicada.

4.1.2. Versió concreta

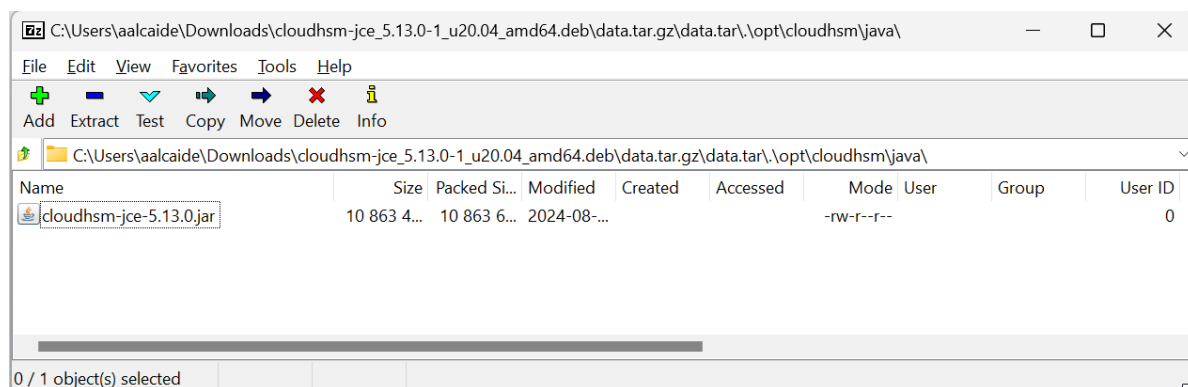
Si volem una versió concreta del JCE provider, vindrem a:

<https://docs.aws.amazon.com/cloudhsm/latest/userguide/client-version-previous.html>

I allà cercarem la versió antiga que ens interessi. La última, actualment només està disponible a latest.

Igual que en el cas anterior, en descomprimir el fitxer .deb, podrem trobar la llibreria java del JCE provider:

```
cloudhsm-jce...._u20.04_amd64.dev > data.tar.gz > data.tar > opt > cloudhsm > java >  
cloudhsm-jce-5.13.0.jar
```



4.2. Instal·lació per compilar el codi

Per poder compilar el codi de PSIS, tant del core com de la consola, hem d'instal·lar aquestes llibreries a un directori concret, així com al repositori maven.

4.2.1. Local

Per treballar en local, en Windows, haurem de copiar la llibreria cloudhsm-jce-X.XX.X.jar a:

```
C:\opt\cloudhsm\java\cloudhsm-jce-X.XX.X.jar
```

I cal instal·lar-la al maven local, doncs no és possible descarregar-la del repositori de maven públic.

Per exemple:

```
mvn install:install-file -Dfile=C:\E\PSIS\PSIS-Cloud\CloudHSM\lib\cloudhsm-jce-5.14.0.jar -DgroupId=com.amazonaws -DartifactId=cloudhsm -Dversion=5.14.0 -Dpackaging=jar
```

4.2.2. Jenkins

Per treballar en local al Jenkins, que és una màquina Linux, haurem de copiar la llibreria cloudhsm-jce-X.XX.X.jar a:

```
/opt/cloudhsm/java/cloudhsm-jce-X.XX.X.jar
```

A la màquina del Jenkins també l'hem d'instal·lar al repositori maven local, pel mateix motiu anterior, i perquè tampoc podem accedir al Code Artifact per descarregar-la (per problemes tècnics d'autenticació pendents de resoldre).

El repositori maven a la màquina del Jenkins es troba al directori:

```
/var/lib/jenkins/.m2/repository/
```

Primer pugem la llibreria per FTP a la carpeta “/home/ubuntu/”.

Un cop pujada per FTP, la instal·larem al repositori maven:

```
cd /opt/apache-maven-3.8.4/bin  
  
sudo ./mvn install:install-file -Dfile=/home/ubuntu/cloudhsm-jce-5.14.0.jar -  
DgroupId=com.amazonaws -DartifactId=cloudhsm -Dversion=5.14.0 -Dpackaging=jar  
  
cd /var/lib/jenkins/.m2/repository/com/amazonaws/cloudhsm  
  
sudo chown -R jenkins:jenkins 5.14.0
```

4.3. Procediment d'actualització

Per actualitzar el JCE provider de CloudHSM, hem de fer lo següent:

- 1) Descarregar la versió que ens interessi.
- 2) Copiar-la al directori "C:\opt\cloudhsm\java\" en local.
- 3) Instal·lar-la manualment al maven local.
- 4) Actualitzar la següent property del pom.xml principal de PSIS:

```
<cloudhsmVersion>5.14.0</cloudhsmVersion>
```
- 5) Comprovar que el codi compila.
- 6) Si no compila, comprovar les APIs, etc...
- 7) Un cop compili en local, actualitzar la llibreria en la màquina Jenkins:
 - Pujar la llibreria per FTP.
 - Copiar-la al directori "/opt/cloudhsm/java/".
 - Instal·lar-la al maven local.
- 8) Generar nova versió de PSIS.
- 9) Generar nova versió de la consola que incorpori la versió de PSIS generada al pas anterior.
- 10) Proves a DEV.