

Configuration d'EJBCA avec LunaSA

PKI crypto

Version 1.0

Le 29/10/2008

Identifiant : DOC_PKI-crypto_Configuration-EJBCA-LunaSA_1.0

Fichier original : DOC_PKI-crypto_Configuration-EJBCA-LunaSA_1.0.odt

Historique des évolutions et visas

Visas

	RÉDACTION	APPROBATION	VALIDATION
NOM	Thomas Chemineau	Bruno Bonfils	Yannick Quenec'hdu
FONCTION	Administrateur Système et Réseau	Chef de Projet	Responsable Département Sécurité
DATE	25/08/2008		
VISA			

Historique des évolutions

L'ajout de son nom par tout nouvel **acteur contributeur** exprime son consentement exprès et non vicié à une distribution du document conforme à la licence indiquée en page 3.

VERSION	DATE	ACTEUR CONTRIBUTEUR	OBJET DE L'ÉVOLUTION
0.1	25/08/2008	Thomas Chemineau	Création
0.2	28/08/2008	David CARELLA	Relecture et corrections
0.3	28/08/2008	Thomas Chemineau	Relecture
1.0	29/10/2008	David CARELLA	Validation

État du document : **60 – En application**

Licence, diffusion et contributeurs

Licence

Ce document est licencié cumulativement sous licences **GNU FDL 1.2** et **CC-BY-SA 3.0**.

La **GNU FDL** est une licence libre copyleft calquée sur la GNU GPL, parfaitement adaptée aux documentations et qui nécessite que soit annexé systématiquement le texte de la licence.

La **CC-BY-SA** est une licence libre copyleft parfaitement adaptée aux contenus multimédias. Sa grande modularité permet de mixer les réalisations.

Cette double licence permet un usage du document qui soit conforme à l'une ou l'autre des licences. Plusieurs avantages peuvent être avancés :

1. Le contenu sous licence est dès lors compatible avec la totalité des licences qui lui sont adjointes ;
2. L'étendue de la double licence est limitée à celle de la licence la plus permissive ;
3. L'utilisation d'au moins une licence française sécurise la double licence au regard des dispositions françaises.

Limitations

Par dérogation au paragraphe précédent, certaines limitations peuvent être apportées à la cession de droits telle que consentie par la licence. Les éléments concernés par ces limitations sont les suivants :

Élément	Titre et/ou description	Licence	Remarque

Diffusion du document

Par dérogation aux paragraphes précédents, la diffusion du document est limitée de la manière qui suit :

Mention de diffusion : **Client du projet**

NOM	ORGANISME	POUR	MÉDIA
Tous les collaborateurs	Groupe Linagora	Information	GED
Collaborateurs du projet		Action	Courriel

Liste des contributeurs

Thomas CHEMINEAU, David CARELLA.

Informations générales

Ordre de lecture (sur fond rouge le document concerné) :

ORDRE	VER.	PROJET	TITRE
01	1.0	3058-01	Installation EJBCA
02	1.0	3058-01	Installation EJBCA haute disponibilité
03	1.0	3058-01	Configuration EJBCA avec appliance LunaSA SafeNet
04	1.0	3058-01	Paramétrage EJBCA

Table des matières

1	Introduction.....	7
2	Conventions.....	8
2.1	Généralités.....	8
2.2	Réseau.....	8
2.3	Spécificité du système.....	8
2.3.1	Comptes et droits utilisateurs.....	9
3	Installation des produits système de LunaSA.....	11
3.1.1	Pré-requis.....	11
3.1.2	Initialisation de l'appliance.....	11
3.1.3	Installation.....	11
4	Configuration de LunaSA.....	13
4.1	Pré-requis.....	13
4.1.1	Régénération du certificat serveur LunaSa.....	13
4.1.2	Création de tokens d'administration.....	13
4.2	Préparation.....	13
4.2.1	Importation du certificat serveur LunaSA.....	13
4.2.2	Enregistrement du cluster HD auprès de l'appliance LunaSA.....	14
4.2.3	Certificat client pour l'authentification LunaSA.....	14
4.3	Création d'une partition LunaSA.....	15
4.4	Associer le cluster HD à une partition LunaSA.....	16
5	Configuration d'EJBCA.....	18
5.1	Re-déploiement d'EJBCA.....	18
5.2	Création d'une clé sur l'appliance LunaSA.....	18
5.3	Création de l'autorité de certification dans EJBCA.....	19
6	Références.....	20

Notations

Le code informatique

Les sorties dans un **terminal** sont représentées ainsi :

```
$ commande1  
# commande2
```

Les commandes à exécuter avec des droits utilisateurs sont précédées du caractère « \$ » tandis que celles à exécuter avec les droits *root* sont précédées du caractère « # ». Ces caractères ne sont pas à saisir dans la ligne de commandes.

Le contenu ou un extrait de **fichier** est représenté ainsi :

```
# Ceci est un exemple de fichier  
parameter1="value"  
parameter2="<NOM-DU-SERVEUR>"
```

Dans le corps de texte, les noms de variables, les extraits de code et les adresses web seront composés en police à chasse fixe. Exemples :

- l'adresse du site web de Linagora est <http://www.linagora.com/> ;
- le contenu de la variable <DATE> est de la forme JJ/MM/AAAA.

Les notes hors texte

Une **remarque** sera représentée de cette façon :

Ceci est un point sur lequel votre attention doit être attirée.

Une **alerte** sera représentée de cette façon :

Ceci est un **point critique** à prendre en compte et pour lequel votre attention est requise.

Les langues étrangères

Les **mots anglo-saxons** sont composés de deux façons : soit en caractères italiques pour les mots du langage courant ou considérés comme tels, soit en caractères droits pour les titres.

Exemples :

Voici un *English text* dans du texte français.
Le protocole Secure Socket Layer est un ...

1 Introduction

Ce document décrit comment créer une autorité de certification dans EJBCA à l'aide de l'appliance LunaSA.

Au préalable, l'architecture haute disponibilité doit être déployée. Dans ce contexte, les instructions qui vont suivre ne sont à appliquer qu'au serveur considéré comme maître dans le *cluster*, étant donné que les données seront automatiquement disponibles sur le SAN distant.

2 Conventions

Quelques conventions de notations supplémentaires sont nécessaires.

2.1 Généralités

L'appliance LunaSA sera dénommée dans la suite de ce document par le terme « LunaSA ».

2.2 Réseau

Voici les conventions d'adressage réseau retenues :

Adresse IP	Nom pleinement qualifié (FQDN)	Description
<VIP>	<VSERVER>	Adresse IP virtuelle du <i>cluster</i> EJBCA en haute disponibilité
<IPLUNA>	<LUNASA>	Information désignant l'appliance LunaSA sur le réseau

Table 2.1 : Convention sur l'adressage réseau

2.3 Spécificité du système

Le système d'exploitation est un système RedHat Enterprise Linux 5.1 qui est un système d'exploitation 64 bits afin de gérer au mieux les grandes capacités mémoire qu'offre la machine.

Arborescence

Différents points de montage sont affectés au SAN, ils sont répartis comme suit :

Répertoire	Description
/bases/pgsql/crpf	Fichiers de la base postgresql et HOME de l'utilisateur « postgres »
/applis/crpf/log	Répertoire de logs
/applis/crpf/back	Répertoire de backup
/applis/crpf/emission	Répertoire de fichiers en émission
/applis/crpf/reception	Répertoire de fichiers en réception

L'application EJBCA installée sur le serveur est articulée autour de l'arborescence suivante

Répertoire	Description
/applis/crpf	Répertoire HOME de l'utilisateur crpfadm
/applis/crpf/bin	Répertoire contenant les binaires et les scripts de l'application
/applis/crpf/etc	Répertoire contenant les fichiers de configuration
/applis/crpf/etc/init.d	Répertoire contenant les scripts de démarrage de l'application
/applis/crpf/bin/ant	Répertoire d'installation de Apache ANT
/applis/crpf/bin/jdk1.6.0_07	Répertoire d'installation de la JDK
/applis/crpf/bin/java	Lien symbolique vers « /applis/crpf/bin/jdk1.6.0_07 »

Répertoire	Description
/applis/crpf/jboss	Répertoire d'installation de JBOSS et HOME de l'utilisateur « jbossadm »

Tableau 2.2: Convention sur les répertoires

2.3.1 Comptes et droits utilisateurs

Dans le cadre du projet CRYPTO plusieurs comptes applicatifs sont créés sur l'ensemble des serveurs liés au projet, des droits spécifiques leurs sont affectés. Ainsi le compte « crpfadm » ayant pour répertoire personnel « /applis/crpf/ » est affecté au projet CRYPTO. Celui-ci doit disposer des droits suivants :

- Bascule vers le compte utilisateur « postgres » via la commande « su » sans mot de passe.
- Arrêt/relance du service « postgresql » et « postgresql_lsb »¹
- Bascule vers le compte utilisateur « jbossadm » via la commande « su »²
- Arrêt/relance du service « jboss »
- Droits d'écriture dans le script de démarrage de jboss
- Droits d'écriture dans les fichiers de configuration de « postgresql »
- Droits d'exécution des scripts de montage et de démontage des systèmes de fichiers du SAN et dédiés à l'application CRYPTO.
- Exécution du binaire de configuration de LunaSA SAFENET « /usr/lunasa/bin/vtl »
- Édition du fichier de configuration « /etc/Chrystoki.conf »

L'ensemble des droits affectés à l'utilisateur « crpfadm » peut être vérifié via la commande :

```
sudo -l
```

Exemple :

```
[crpfadm@HCRPLX01 ~]$ sudo -l
User crpfadm may run the following commands on this host:
[...]
(root) NOPASSWD: /bin/su - postgres
(root) NOPASSWD: /etc/init.d/postgresql *
(root) NOPASSWD: /etc/init.d/postgresql_lsb *
(root) NOPASSWD: /bin/su - jbossadm
(root) NOPASSWD: /etc/init.d/jboss *
(root) NOPASSWD: /etc/init.d/jboss *
(root) NOPASSWD: /applis/crpf/demontage.sh
(root) NOPASSWD: /applis/crpf/montage.sh
(root) NOPASSWD: /usr/lunasa/bin/vtl
(root) NOPASSWD: /bin/vi /etc/Chrystoki.conf
```

Afin de faire fonctionner le serveur de servlet JBOSS un utilisateur spécifique est créé, il s'agit

- 1 Script spécifique d'arrêt/relance de postgresql créé ultérieurement afin de rendre compatible le système de démarrage du SGBD avec le programme Heartbeat (cf. 3058-01_DOC_PKI-crypto_Installation-HD_1.0)
- 2 Compte spécifique d'exécution du serveur de servlet JBoss

de l'utilisateur « jbossadm » ayant pour répertoire personnel « /applis/crpf/bin/jboss ». Ce répertoire est créé lors de l'installation du serveur de servlet.

3 Installation des produits système de LunaSA

L'installation des pilotes (*drivers*) de l'appliance Luna SafeNet est nécessaire afin qu'EJBCA puisse l'utiliser. Ce chapitre décrit succinctement leur installation.

3.1.1 Pré-requis

Au préalable, veuillez copier l'intégralité du CD-ROM d'installation dans le répertoire `/applis/crpf/sources/lunasa`. Les patches livrés doivent être copiés dans le répertoire `/applis/crpf/sources/lunasa/linux`, sous la forme d'un fichier d'extension « `.zip` » (nommé `008977-002.zip` lors de la rédaction de ce document).

3.1.2 Initialisation de l'appliance

L'initialisation de l'appliance s'effectue naturellement grâce à la documentation fournie par SafeNet, disponible sur le CD-ROM. Pour cette appliance, le réseau doit être correctement configuré (adressage IP statique), et la résolution DNS doit être fonctionnelle. Ce document n'aborde que l'installation des pilotes (*drivers*) sous Linux pour la prise en charge de l'appliance par EJBCA.

3.1.3 Installation

Avant toute chose, il faut déployer les patches mis à disposition par SafeNet :

```
# cd /applis/crpf/sources/lunasa/linux
# unzip 008977-002.zip
# cd ./64
```

En toute logique, les deux sous-répertoires « `32` » et « `64` » doivent être correctement complétés. Les fichiers suivants doivent être modifiés pour insérer l'option « `--nodeps` » à chaque commande d'installation RPM :

```
/applis/crpf/sources/lunasa/linux/64/install.sh
/applis/crpf/sources/linux/64/javasp/install_lunajsp.sh
```

Ainsi, par exemple, la commande « `rpm -i $pkg` » devient « `rpm -i --nodeps $pkg` ».

Une fois les fichiers corrigés, il faut lancer l'installation via un compte utilisateur disposant des droits « `root` » ou dont les droits d'exécution via la commande « `sudo` » ont été correctement établis :

```
$ sudo ./install.sh ##### ou "# ./install.sh " si le compte "root" est utilisé
[...]
If you select 'no' or 'n', this product will not be installed.
(y/n) y

Installed configurator-4.2.0-7.x86_64.rpm
Checking for /etc/Chrystoki.conf.rpmsave
Using new /etc/Chrystoki.conf
/etc/Chrystoki.conf is up to date.
Installed libcryptoki-4.2.0-7.x86_64.rpm
Installed vtl-4.2.0-7.x86_64.rpm
Installed ckdemo-4.2.0-7.x86_64.rpm
Installed multitoken-4.2.0-7.x86_64.rpm
```

```

Installed salogin-4.2.0-7.x86_64.rpm
Installed ctp-4.2.0-7.x86_64.rpm
Installed libshim-4.2.0-7.x86_64.rpm
Installed lunacmu-4.2.0-7.x86_64.rpm
Would you like to install the Luna JSP for Luna SA? (y/n)
y
Installed lunajsp-4.2.0-7.x86_64.rpm
Installed lunajmt-4.2.0-7.x86_64.rpm
Installation of the Luna JSP for Luna SA - Release 4.2.0-7 successful.

../../docs/readme.txt: Aucun fichier ou répertoire de ce type

Installation of the Luna SA Client Software - Release 4.2.0-7 successful.

Would you like to install the SDK for Luna SA? (y/n)
n
If you wish to install the SDK for Luna SA at a later time, simply run
install_lunasdk.sh in the SDK directory.

```

Les paquets RPM suivants ont normalement été installés avec succès :

- **libcryptoki-4.2.0-7 ;**
- **ckdemo-4.2.0-7 ;**
- **salogin-4.2.0-7 ;**
- **libshim-4.2.0-7 ;**
- **lunajsp-4.2.0-7 ;**
- **configurator-4.2.0-7 ;**
- **vt1-4.2.0-7 ;**
- **multitoken-4.2.0-7 ;**
- **ctp-4.2.0-7 ;**
- **lunacmu-4.2.0-7 ;**
- **lunajmt-4.2.0-7.**

Sur les systèmes RedHat Enterprise Linux 5.x, il se peut qu'il y ait une erreur sur l'outil **vt1** fourni par les paquets RPM installés. Généralement, elle s'est résolue en installant aussi le paquet système **libstdc++2.10-glibc2.2**.

4 Configuration de LunaSA

Ce chapitre décrit les étapes de configuration à effectuer afin que le système puisse communiquer avec l'appliance LunaSA.

L'appliance LunaSA doit être disponible sur le réseau, et complètement opérationnelle.

4.1 Pré-requis

4.1.1 Régénération du certificat serveur LunaSa

Il est conseillé de régénérer le certificat serveur par défaut de l'appliance. Pour cela, il est nécessaire d'ouvrir une connexion SSH sur l'appliance. Une fois authentifié, la commande suivante permet de régénérer un tel certificat :

```
lunash:> sysconf regenCert
CAUTION: Current Server Certificate and Private Key will be
overwritten. All clients will have to add the server
again with new certificate.
Type 'proceed' to generate cert or 'quit' to cancel
> proceed
lunash:>
```

4.1.2 Création de tokens d'administration

Voir la documentation constructeur de LunaSA.

4.2 Préparation

Il s'agit désormais de préparer le serveur à pouvoir communiquer avec l'appliance LunaSA. Pour cela, la documentation fournie par le constructeur est très complète. Voici néanmoins les étapes de configuration qu'il est conseillé d'effectuer dans le cadre du projet.

4.2.1 Importation du certificat serveur LunaSA

Il faut s'assurer que le répertoire `/usr/lunasa/bin` existe. Il s'agit d'une architecture de haute disponibilité, le répertoire est présent sur le serveur maître du *cluster*.

L'utilisateur applicatif du projet « crypto », doit disposer des droits d'exécution via « sudo » sur l'ensemble des exécutables présents dans le répertoire `/usr/lunasa/bin` ainsi que les droits d'édition sur le fichier « `/etc/Chrystoki.conf` »

```
$ cd /usr/lunasa/bin
$ sudo ./ctp admin@<IPLUNA>:server.pem ./
[...]
$ ls -l | grep server.pem
-rw-r--r-- 1 root root      822 2008-07-31 15:32 server.pem
```

À noter qu'il faut remplacer la variable `<IPLUNA>` par l'adresse IP de l'appliance LunaSA au sein du réseau. De plus, le mot de passe du compte « `admin` », si l'appliance n'a pas été initialisée, est le mot « `chrysalis` ».

4.2.2 Enregistrement du *cluster* HD auprès de l'appliance LunaSA

Il faut invoquer la commande `vt1` avec le paramètre « `addServer` », afin d'enregistrer le serveur EJBCA auprès de l'appliance LunaSA.

```
$ cd /data/usr/lunasa/bin
$ sudo ./vt1 addServer -n <VIP> -c server.pem

New server <VIP> successfully added to server list.
```

Remarques à propos de la commande précédente :

- le but est d'enregistrer auprès de l'appliance LunaSA l'adresse IP virtuelle `<VIP>` du *cluster* haute disponibilité ;
- une erreur peut subvenir à l'exécution de la commande `vt1` sur les systèmes RedHat Enterprise Linux 5 ; en générale, celle-ci peut être résolue par l'installation du paquet `libstdc++2.10-glibc2.2`.

4.2.3 Certificat client pour l'authentification LunaSA

En premier lieu, il s'agit de créer le certificat du serveur :

```
$ cd /usr/lunasa/bin
$ ./vt1 createCert -n <VIP>
Private Key created and written to: /usr/lunasa/cert/client/<VIP>Key.pem
Certificate created and written to: /usr/lunasa/cert/client/<VIP>.pem
$ ls -f /usr/lunasa/cert/client
total 8
-rw-r--r-- 1 root root 963 2008-07-31 15:33 <VIP>Key.pem
-rw-r--r-- 1 root root 818 2008-07-31 15:33 <VIP>.pem
```

Ensuite, il faut l'exporter vers l'appliance LunaSA :

```
$ cd /usr/lunasa/bin
$ ./ctp /data/usr/lunasa/cert/client/<VIP>.pem admin@<IPLUNA>:
```

Pour terminer cette étape, il est nécessaire d'enregistrer le client sur l'appliance LunaSA, en ouvrant une session SSH sur l'appliance, en tant qu'administrateur. La commande s'utilise ainsi :

```
lunash:> client -register -client <CLIENT'S-NAME> -hostname <CLIENT'S-HOSTNAME>
```

Ce qui se traduit donc par la commande suivante :

```
lunash:> client -register -client ejbcacluster -hostname <VIP>
lunash:> client list
registered client 1: ejbcacluster

Command Result : 0 (Success)
```

4.3 Création d'une partition LunaSA

Dans les exemples qui suivent, la partition créée sera nommée « `ejbcapartition` ».

Le but est de créer une partition sur l'appliance LunaSA qui contiendra les clés et les certificats de l'autorité de certification. Pour ce faire, il est nécessaire de se connecter à l'appliance par SSH via le compte d'administration, puis de procéder à une authentification par token d'administration sur l'appliance :

```
lunash:> hsm login
```

L'appliance requiert le token d'administration, et une authentification réussie sur le PED (PIN Entry Device) connecté à l'appliance.

Ensuite, il est possible de créer une partition manuellement :

```
lunash:> partition -create -name ejbcapartition
```

L'appliance LunaSA demande ensuite un token vierge afin de l'initialiser pour la partition en cours de création. Ce token servira par la suite à accéder aux clés de la partition. Comme le précise la documentation de l'appliance :

- insérer un token vierge, puis presser la touche « **ENT** » sur le PED ;
- le PED demande s'il s'agit d'un token de groupe, choisir « **YES** » ou « **NO** » ;
- saisir ensuite deux fois un mot de passe pour ce token, puis presser la touche « **ENT** » ;
- le PED indique s'il faut dupliquer le token, choisir « **YES** » ou « **NO** ».

Le PED génère ensuite aléatoirement un mot de passe pour la partition. Ce mot de passe doit être noté scrupuleusement ; il sera réutilisé par la suite. Voici un exemple de ce qui doit s'afficher sur le PED, où le mot de passe apparaît en caractères gras :

```
Login secret value
btqx-EFGH-3456-7/K9
Please write it down.
(Press ENTER)
```

Il est impératif de retenir le mot de passe : il ne sera pas possible de le re-demander à l'appliance. Ce mot de passe est très important pour la suite des opérations. Par ailleurs, il ne faut pas oublier que l'opération de partition possède un *timeout* d'une minute. Au delà de ce délai d'une minute (par exemple pour retenir le mot de passe), l'opération échouera.

Dans la console de l'appliance LunaSA, un message de succès doit s'afficher. Il est possible de contrôler que la partition est bien présente :

```
[...]
partition create successful
lunash:> partition list

Partition: 950956001,      Name: ejbcapartition

Command Result : 0 (Success)
```

4.4 Associer le *cluster* HD à une partition LunaSA

Il faut associer le *cluster* de haute disponibilité à une partition de l'appliance. Cette action se fait toujours dans une session SSH sur l'appliance :

```
lunash:> client assignPartition -client ejbcacluster -partition ejbcapartition
lunash:> client show -client ejbcacluster

ClientID:      ejbcacluster
Hostname:     <VIP>
Partitions:   "ejbcapartition"

Command Result : 0 (Success)
```

Il faut impérativement vérifier que tout fonctionne correctement depuis le serveur. Il ne faut pas oublier que l'appliance est accédée via l'adresse IP virtuelle, puisque cette adresse IP est utilisée lors de la génération des certificats client. Si ce n'est pas le cas, une erreur surviendra :

```
$ cd /usr/lunasa/bin
$ sudo ./vtl verify

Error: Unable to find any Luna SA slots/partitions among registered
servers. Ensure this client is assigned partitions on the
Luna SA servers, and check the vtl supportInfo command for
other possible problems such as unable to ping a server, or
missing configuration files.
```

Une simple règle **iptables** peut résoudre en principe le problème, celle-ci doit être renseignée par l'administrateur du système (« root ») :

```
# iptables -t nat -A POSTROUTING -o eth0 -d <IPLUNA> -j SNAT --to-source <VIP>
```

```
$ cd /usr/lunasa/bin
$ sudo ./vtl verify

The following Luna SA Slots/Partitions were found:

Slot Serial #      Label
==== ===========  =====
  1   950956001    ejbcapartition
```

La règle **iptables** précédente doit impérativement être fixée à chaque démarrage du système.

Si l'erreur survient toujours, il se peut que des informations soient manquantes dans le fichier **/etc/Chrystoki.conf**. En pratique, il faut que le fichier ressemble à ce qui suit :

```
Chrystoki2 = {
    LibUNIX64=/data/usr/lib/libCryptoki2_64.so;
}
Luna = {
    DefaultTimeOut=500000;
    PEDTimeout1=100000;
    PEDTimeout2=100000;
}
```

```
CardReader = {
  RemoteCommand=1;
}
LunaSA Client = {
  ClientPrivKeyFile = /data/usr/lunasa/cert/client/<VIP>Key.pem;
  ClientCertFile = /data/usr/lunasa/cert/client/<VIP>.pem;
  ServerPort00 = 1792;
  ServerName00 = <VIP>;
  ServerPort01 = 1792;
  ServerName01 = <IPLUNA>;
  NetClient=1;
  ServerCAFile=/data/usr/lunasa/cert/server/CAFile.pem;
  SSLConfigFile=/data/usr/lunasa/bin/openssl.cnf;
  ReceiveTimeout=20000;
}
```

5 Configuration d'EJBCA

Ce chapitre décrit comment configurer EJBCA afin qu'il puisse s'adresser à l'appliance LunaSA correctement.

5.1 Re-déploiement d'EJBCA

Les pilotes Java doivent être correctement installés. Ainsi, une fois JBoss installé, il s'agira de copier les fichiers JAR adéquats dans le répertoire `/applis/crpf/bin/jboss/server/default/lib` :

```
$ sudo su - jbossadm
$ cp /usr/lunasa/jsp/lib/*.jar /applis/crpf/bin/jboss/server/default/lib.
```

Il en va de même pour EJBCA :

```
$ cp /usr/lunasa/jsp/lib/*.jar /applis/crpf/ejbca/lib
```

Il faut désormais obligatoirement activer l'option `hsm.luna=X` dans le fichier de configuration d'EJBCA, soit `/applis/crpf/ejbca*/conf/ejbca.properties`.

Ensuite, selon le guide d'installation d'EJBCA [`EJBCA:INSTALL`], il s'agit de re-déployer EJBCA dans JBoss :

```
$ cd $EJBCA_HOME
$ ant deploy
```

Le service JBoss doit être arrêté avant d'exécuter la commande précédente.

Si le déploiement s'est correctement effectué, il est nécessaire de démarrer de nouveau le service JBoss du système.

5.2 Création d'une clé sur l'appliance LunaSA

Cette opération est importante. EJBCA a été déployée avec le support LunaSA. Un outil est proposé par EJBCA afin d'interagir avec l'appliance, notamment pour l'opération de création de clé. Cet outil s'utilise comme suit :

```
$ ./lunaHSM.sh generate keyLabel keyLength partitionName partitionPassword
```

Le mot de passe de la partition est celui affiché par le PED LunaSA lors de la création de la partition. Il est de la forme « `btqx-EFGH-3456-7/K9` », et sera utilisé sans les caractères « - ».

```
$ cd $EJBCA_HOME/bin
$ ./lunaHSM.sh generate defaultKey 4096 ejbcapartition btqxEFGH34567/K9
Number of Slots: 1
Slot: 1 Token Label: ejbcapartition
```

Dès à présent, l'appliance demande le token d'authentification associé à la partition. Il faut l'insérer dans le PED, puis valider le mot de passe pour s'authentifier avec succès.

Si tout s'est correctement passé, l'appliance devrait afficher ce qui suit :

```
Loading Luna Keystore
Storing certificate with entry defaultKey via KeyStore
```

5.3 Création de l'autorité de certification dans EJBCA

Dans l'interface d'administration d'EJBCA, il s'agit de se rendre sur la page de création d'une nouvelle autorité de certification. Une fois le formulaire de création affiché, il faut :

- sélectionner « SafeNetLunaCAToken » dans la liste déroulante désignée par le libellé « CA Token Type » ;
- saisir les informations suivantes dans le champ « Hard CA Token Properties » :

```
slotLabel ejbca
defaultKey defaultKey
```

- saisir le code d'authentification, qui correspond en fait au mot de passe de la partition, celui-là même entré lors de la création de la clé lors de l'étape précédente ;
- choisir un « subject DN », par exemple « cn=SogeraCA » ;
- choisir une durée de validité en jours, par exemple « 3653 » (10 ans).

Lorsque le formulaire est correctement rempli, il reste à valider à l'aide du bouton « create ».

À cet instant, l'appliance Luna SafeNet demande le token de la partition pour authentification. Il faut l'insérer dans le PED et saisir les informations demandées.

Si l'authentification est un succès, la création de l'AC sera effective et sans message d'erreur.

6 Références

Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE
EJBCA : INSTALL	1.0	3058-01	Assistance EJBCA – Guide d'installation

Références externes

RÉFÉRENCE	VER.	ÉDITEUR	TITRE

Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB