



# Module 1 – Installation

## Formation EJBCA

EJBCA 3.6 et supérieures [fr]

Version 1.1

Le 26/06/2009

Nom du fichier : 9999-02\_SF\_Formation-EJBCA\_Module-1-Installation\_1.1

## Historique des évolutions et visas

### Visas

	RÉDACTION	APPROBATION	VALIDATION
<b>NOM</b>	David CARELLA		
<b>FONCTION</b>	Expert PKI		
<b>DATE</b>			
<b>VISA</b>			

### 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	06/06/2008	David CARELLA	Création. Structure du document basé sur le document original en anglais et sur le Guide d'installation en français.
0.2	13/06/2008	David CARELLA	Traduction.
0.3	17/06/2008	André PELLÉ	Corrections.
0.4	23/06/2008	David CARELLA	Mise à jour : sigles, droits.
0.5	25/06/2008	David CARELLA	Intégration des mises à jour d'André PELLÉ.
1.0	26/06/2008	David CARELLA	Version finale (validation).
1.1	26/06/2009	David CARELLA	Mise à jour : EJBCA 3.8, Java 6

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

## Licence, diffusion et contributeurs

### Licence

Ce document est licencié cumulativement sous licences **GNU FDL 1.3** 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 : Groupe Linagora**

NOM	ORGANISME	POUR	MÉDIA

### Liste des contributeurs

Auteurs originaux de la version anglaise : Joakim BÅGNERT, Henrik ANDREASSON.

Auteurs traducteurs de la version française : David CARELLA, André PELLÉ.

## Table des matières

<b>1</b>	<b>Introduction.....</b>	<b>7</b>
<b>1.1</b>	<b>Objectifs.....</b>	<b>7</b>
1.1.1	Cible.....	7
1.1.2	But.....	7
<b>1.2</b>	<b>Pré-requis.....</b>	<b>7</b>
1.2.1	Connaissances requises.....	7
1.2.2	Pré-requis matériels.....	7
<b>1.3</b>	<b>Durée.....</b>	<b>7</b>
<b>2</b>	<b>Présentation de cette formation.....</b>	<b>8</b>
<b>3</b>	<b>Caractéristiques d'EJBCA.....</b>	<b>9</b>
<b>3.1</b>	<b>Systèmes d'exploitation supportés.....</b>	<b>9</b>
3.1.1	GNU/Linux.....	9
3.1.2	Windows.....	9
3.1.3	UNIX.....	9
<b>3.2</b>	<b>Versions de Java.....</b>	<b>9</b>
<b>3.3</b>	<b>Serveurs d'applications supportés.....</b>	<b>9</b>
3.3.1	JBoss.....	9
3.3.2	WebLogic.....	10
3.3.3	GlassFish.....	10
<b>3.4</b>	<b>Bases de données supportées.....</b>	<b>10</b>
3.4.1	MySQL.....	10
3.4.2	PostgreSQL.....	10
3.4.3	HSQLDB (Hypersonic).....	10
3.4.4	Oracle.....	10
3.4.5	Sybase SQL Anywhere.....	11
3.4.6	MS-SQL2000.....	11
3.4.7	Informix.....	11
3.4.8	Derby.....	11
<b>4</b>	<b>Installation d'EJBCA.....</b>	<b>12</b>
<b>4.1</b>	<b>Pré-requis pour ce cours.....</b>	<b>12</b>
<b>4.2</b>	<b>Installation du système d'exploitation.....</b>	<b>12</b>
<b>4.3</b>	<b>Configuration « sudo ».....</b>	<b>13</b>
4.3.1	Création de l'utilisateur « ejbca ».....	13
4.3.2	Configuration de l'outil « sudo ».....	13
4.3.3	Préparations des fichiers d'installation.....	14
<b>4.4</b>	<b>Installation de la base de données.....</b>	<b>14</b>
4.4.1	Installation de MySQL.....	14
4.4.2	Démarrage automatique de MySQL.....	14
4.4.3	Vérification de l'installation de MySQL.....	14
<b>4.5</b>	<b>Installation de Java et JCE.....</b>	<b>15</b>
<b>4.6</b>	<b>Installation du serveur d'applications.....</b>	<b>16</b>
4.6.1	Installation de JBoss.....	16
<b>4.7</b>	<b>Installation de Ant.....</b>	<b>17</b>

<b>4.8</b>	<b>Installations spécifiques.....</b>	<b>17</b>
4.8.1	Installation du pilote MySQL pour JBoss.....	17
<b>4.9</b>	<b>Installation de l'application EJBCA.....</b>	<b>18</b>
<b>5</b>	<b>Configuration d'EJBCA.....</b>	<b>19</b>
<b>5.1</b>	<b>Variables d'environnement.....</b>	<b>19</b>
<b>5.2</b>	<b>Création de la base de données et du compte « ejbca ».....</b>	<b>19</b>
5.2.1	Création de la base de données MySQL.....	19
5.2.2	Création du compte utilisateur MySQL « ejbca3 ».....	20
<b>5.3</b>	<b>Fichiers de configuration d'EJBCA.....</b>	<b>20</b>
5.3.1	Fichier « ejbca.properties ».....	20
5.3.2	Fichier « database.properties ».....	21
5.3.3	Fichier « web.properties ».....	22
5.3.4	Autres fichiers de propriétés.....	22
<b>5.4</b>	<b>Démarrage d'EJBCA.....</b>	<b>23</b>
5.4.1	Arrêt du serveur d'applications JBoss.....	23
5.4.2	Changement de propriétaires des fichiers installés.....	23
5.4.3	Initialisation d'EJBCA : tâche « Bootstrap ».....	23
5.4.4	Démarrage du serveur d'applications JBoss.....	24
5.4.5	Installation d'EJBCA.....	25
5.4.6	Initialisation du magasin de clés « javastruststore ».....	26
5.4.7	Arrêt du serveur d'applications JBoss.....	27
5.4.8	Déploiement d'EJBCA.....	27
5.4.9	Démarrage du serveur d'applications JBoss.....	27
<b>5.5</b>	<b>Démarrage de la console d'administration web.....</b>	<b>28</b>
5.5.1	Importation du certificat « SuperAdmin » dans un navigateur.....	28
5.5.2	Démarrage de l'administration web d'EJBCA.....	28
<b>6</b>	<b>Initialisation de l'IGC.....</b>	<b>29</b>
<b>6.1</b>	<b>Service de publication LDAP.....</b>	<b>29</b>
6.1.1	Création du service de publication.....	29
6.1.2	Édition du service de publication.....	29
<b>6.2</b>	<b>Service de publication OCSP.....</b>	<b>29</b>
6.2.1	Création du service de publication.....	29
6.2.2	Édition du service de publication.....	30
6.2.3	Création du profil de certificats OCSPSigner.....	30
<b>6.3</b>	<b>Validation et tests de bon fonctionnement.....</b>	<b>30</b>
6.3.1	Ajout d'un nouvel utilisateur.....	31
6.3.2	Émission du certificat utilisateur.....	31
6.3.3	Exportation d'un certificat d'AC.....	32
6.3.4	Ajout d'un certificat d'AC dans Apache.....	32
<b>7</b>	<b>Compléments.....</b>	<b>33</b>
<b>7.1</b>	<b>Introduction à la cryptographie.....</b>	<b>33</b>
<b>7.2</b>	<b>Prochaines étapes après ce cours.....</b>	<b>33</b>
<b>8</b>	<b>Sigles et acronymes.....</b>	<b>34</b>
<b>9</b>	<b>Références documentaires.....</b>	<b>37</b>

## 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 est un **support de formation** à EJBCA. Il contient des sujets traitant de l'**installation d'EJBCA** pour divers environnements.

## 1.1 Objectifs

---

### 1.1.1 Cible

Toute personne intégrateur, exploitant et/ou administrateur de systèmes GNU/Linux.

### 1.1.2 But

Être capable d'installer une IGC basée sur l'application EJBCA pour plusieurs environnements logiciels et matériels.

## 1.2 Pré-requis

---

### 1.2.1 Connaissances requises

Afin d'aborder cette formation dans de bonnes conditions, il est recommandé que vous ayez les connaissances suivantes :

- les bases de l'administration GNU/Linux ;
- les concepts de base des IGC (infrastructures de gestion de clés).

### 1.2.2 Pré-requis matériels

Le besoin en matériel est le suivant :

- une salle équipée d'un vidéo projecteur ;
- un poste de travail par stagiaire.

## 1.3 Durée

---

En pleine possession des connaissances pré-requises, cette formation durera environ un jour.

## 2 Présentation de cette formation

Dans ce cours, nous allons installer EJBCA dans un système d'exploitation standard.

EJBCA sera configuré à l'aide d'un certificat d'AC logiciel. Ce qui n'est pas recommandé pour une configuration de production requérant un haut niveau de sécurité.

L'utilisation d'une AC sur support matériel est décrite dans le cours « Module 3 – Utilisations avancées ».

Nous allons utiliser une base de données ayant fait ses preuves dans le monde de l'entreprise. MySQL qui est capable de faire de la réplication, sera utilisée comme une simple base de données.

## 3 Caractéristiques d'EJBCA

Ce chapitre présente une vue d'ensemble de tous les environnements sur lesquels EJBCA peut être déployé.

### 3.1 Systèmes d'exploitation supportés

EJBCA peut être exécuté sur tous les systèmes d'exploitation qui supportent Java et les serveurs d'applications J2EE.

#### 3.1.1 GNU/Linux

EJBCA a été testée sur :

- Suse Linux Enterprise Server, versions : 9, 10 ;
- Debian Sarge (3.1), Debian Etch (4.0) et Debian Lenny (testing) ;
- Ubuntu, versions : 6.06, 6.10, 8.04.

#### 3.1.2 Windows

- Windows 2003 Server ;
- Windows XP.

#### 3.1.3 UNIX

- Solaris 9 ;
- MacOS X ;
- OpenBSD 4.0 (sans XKMS).

## 3.2 Versions de Java

Tous les cours ainsi que toutes les installations connues utilisent l'environnement Java de SUN en version 1.4.2, 1.5, 1.6.

À la date d'aujourd'hui (juin 2009), la version à choisir est la **version 1.6**.

## 3.3 Serveurs d'applications supportés

EJBCA supporte les **serveurs d'applications J2EE** suivants.

Pour plus d'informations à propos des serveurs d'applications J2EE, consultez la page suivante : <http://fr.wikipedia.org/wiki/J2EE>

#### 3.3.1 JBoss

Le serveur d'applications **JBoss** utilisé par les développeurs d'EJBCA est le choix recommandé si vous vous n'êtes pas spécialement intéressés à d'autres serveurs d'applications.

<http://www.jboss.org/>

### 3.3.2 WebLogic

Le serveur d'applications **WebLogic** est supporté avec une base de données Oracle.

[http://commerce.bea.com/products/weblogicplatform/weblogic\\_prod\\_fam.jsp](http://commerce.bea.com/products/weblogicplatform/weblogic_prod_fam.jsp)

### 3.3.3 GlassFish

**GlassFish** est un serveur J2EE produit par SUN et récemment supporté.

<http://java.sun.com/javaee/community/glassfish/>

## 3.4 Bases de données supportées

### 3.4.1 MySQL

**MySQL** est la base de données utilisée pour le développement d'EJBCA. Donc, si vous n'êtes pas spécialement intéressés à d'autres bases de données, c'est probablement le meilleur choix. MySQL est aussi la base de données la plus déployée parmi les utilisateurs d'EJBCA. Avec MySQL vous pouvez configurer un solution de réplication maître à haut niveau de redondance.

**Les versions testées :** 4.1 et 5.0

Pour plus d'informations à propos de MySQL, consultez : <http://www.mysql.com/>

### 3.4.2 PostgreSQL

**PostgreSQL** est un puissant système de base de données relationnel Open Source.

**Les versions testées :** 7.2 et 8.0

Pour plus d'informations à propos de PostgreSQL, consultez : <http://www.postgresql.org/>

### 3.4.3 HSQLDB (Hypersonic)

**HSQLDB** – basée sur le projet Hypersonic – est la base de données par défaut dans JBoss. Elle est également incluse dans la suite bureautique OpenOffice.org 2.0.

Dans un environnement de production, il est recommandé de ne pas utiliser la base de données HSQLDB (Hypersonic) fournie par défaut dans JBoss pour les raisons suivantes :

1. La base de données HSQLDB est en mémoire : cela signifie qu'elle consomme de plus en plus de mémoire au fil du temps. Si un grand nombre de certificats est émis, les émissions prendront un temps conséquent ;
2. HSQLDB ne supporte pas entièrement SQL, en particulier les états ALTER. Lorsqu'une nouvelle version d'EJBCA est publiée, les scripts ne seront pas mis à jour selon tel ou tel changement de table dans la base.

Pour plus d'informations à propos de HSQLDB (Hypersonic), consultez : <http://hsqldb.org/>

### 3.4.4 Oracle

**Oracle** Database 10g Enterprise Edition offre des performance pour les entreprises, évolutivité et fiabilité pour des configurations en *cluster* ou en simple serveur. Elle fournit des caracté-

ristiques pour supporter la plupart des applications de traitement de transactions, d'intelligence économique et de gestion de contenus.

**Les versions testées :** 8i, 9i et 10i

Pour plus d'informations à propos d'Oracle, consultez : <http://www.oracle.com/>

Vous pouvez aussi consulter : [http://en.wikipedia.org/wiki/Oracle\\_database](http://en.wikipedia.org/wiki/Oracle_database)

### 3.4.5 Sybase SQL Anywhere

**SQL Anywhere®** de la société Sybase.

<http://www.sybase.com/products/databasemanagement/sqlanywhere>

Pour plus d'informations, consultez : <http://en.wikipedia.org/wiki/Sybase>

### 3.4.6 MS-SQL2000

**Microsoft SQL Server.**

**Les versions testées :** 2000 et 2005

Pour plus d'informations, consultez : <http://www.microsoft.com/sql/>

### 3.4.7 Informix

IBM® **Informix®** Dynamic Server Express.

**Les versions testées :** 9.2

Pour plus d'informations : <http://www-306.ibm.com/software/data/informix/ids-express/>

### 3.4.8 Derby

**Derby** est la base de données par défaut dans le serveur d'applications GlassFish.

Apache Derby, un sous-projet base de données d'Apache, est une base de données relationnelle Open Source entièrement implémentée en Java et disponible sous la licence Apache version 2.0. Les principaux avantages sont :

- Derby est de petite taille en mémoire – environ deux mégaoctets pour le moteur et le pilote JDBC inclus ;
- Derby est basée sur Java, JDBC et les standards SQL ;
- Derby fournit un pilote JDBC inclus qui vous permet d'intégrer Derby dans toute solution basée sur Java ;
- Derby supporte également le mode client/serveur avec le pilote JDBC client Derby et le serveur Derby ;
- Derby est simple à installer, à déployer et à utiliser.

Si vous découvrez Derby, veuillez consulter la page « Quick Start » sur le site web de Derby.

Pour plus d'informations à propos de Derby, consultez : <http://db.apache.org/derby/>

## 4 Installation d'EJBCA

Dans ce chapitre, nous allons installer toutes les parties nécessaires pour déployer EJBCA.

### 4.1 Pré-requis pour ce cours

Nous allons utiliser :

- un système d'exploitation client : Ubuntu ou Windows XP ;
- un système d'exploitation serveur pour la PKI : DEBIAN ou Ubuntu ;
- une base de données : MySQL 5.0 ;
- un serveur d'applications : JBoss 4.2.3 ;
- un connecteur Java MySQL : MySQL Java connector 5.1.7 ;
- un système de construction : Ant 1.7.1 ;
- une infrastructure de gestion de clés : EJBCA 3.8.3.

**Remarque :** tous les logiciels nécessaires sont dans le répertoire `/home/ejbca`.

Pour ce cours, nous utiliserons les notations de versions suivantes :

JBoss `<VERSION-JBOSS>`

Ant `<VERSION-ANT>`

### 4.2 Installation du système d'exploitation

**Remarque :** cette étape peut être facultative, selon l'environnement logiciel de la formation.

Le système d'exploitation est fourni dans ce cours.

Démarrez le serveur et connectez vous avec l'utilisateur `ejbca` et le mot de passe `ejbca`.

En cas d'urgence, utiliser le compte `root` avec le mot de passe `foo123`.

Pour passer en `root` saisir : `sudo su -`

Démarrez le serveur, puis vérifiez son adresse IP avec la commande `/sbin/ifconfig`.

Maintenant, ouvrez le fichier :

```
c:\windows\system32\drivers\etc\hosts
/etc/hosts
```

... et insérez l'adresse IP et le nom d'hôte du serveur EJBCA :

```
<ADRESSE-IP> <NOM-DU-SERVEUR-EJBCA>
```

Par exemple :

```
192.168.156.128 <NOM-DU-SERVEUR-EJBCA>
```

Après vous êtes connecté au serveur avec SSH, vous serez prêt pour la prochaine partie de l'installation.

## 4.3 Configuration « sudo »

Avant de commencer l'installation, il va falloir ajouter un utilisateur et configurer le fichier « `/etc/sudoers` » afin d'avoir la possibilité d'exécuter certaines commandes avec les droits « `root` ». Cette partie traite de la marche à suivre pour créer l'utilisateur « `ejbca` » et lui fournir les privilèges avec l'outil `sudo`.

### 4.3.1 Création de l'utilisateur « `ejbca` »

La création d'un utilisateur se fait de la manière suivante :

```
jboss@server:~# adduser ejbca
Enter new UNIX password:
Retype new UNIX password:
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur jboss
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
  Nom complet []:
  N° de bureau []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Ces informations sont-elles correctes ? [o/N] o
jboss@server:~# su ejbca
Password:
```

### 4.3.2 Configuration de l'outil « `sudo` »

La configuration de l'outil « `sudo` » pour l'utilisateur « `ejbca` » se fait de la manière suivante.

Exécutez la commande « `visudo` » pour éditer le fichier « `/etc/sudoers` » :

```
ejbca@server:~$ visudo
```

Éditer le fichier en ajoutant les deux dernières lignes de cet exemple :

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults            env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Spécification des privilèges de l'utilisateur ejbca
ejbca   ALL=(ALL) ALL
```

### 4.3.3 Préparations des fichiers d'installation

Afin de réaliser l'installation de manière propre, il est recommandé de disposer de deux répertoires. Le premier permettra de télécharger et stocker les sources et les binaires d'installation et le second sera utilisé pour l'installation des composants.

Dans la suite de cette formation, nous nommerons « `sources` » le fichier contenant les fichiers téléchargés et « `tools` » celui contenant l'installation.

```
ejbca@server:~$ sudo mkdir /opt/sources
ejbca@server:~$ sudo chown ejbca:ejbca /opt/sources
ejbca@server:~$ sudo mkdir /opt/tools
ejbca@server:~$ sudo chown ejbca:ejbca /opt/tools
```

## 4.4 Installation de la base de données

La base de données contiendra toutes les informations créées par EJBCA, telles que les certificats, les LCR (liste des certificats révoqués) et toutes les informations à propos des utilisateurs. Même les AC ayant un support logiciel seront stockées dans la base de données. Dans un environnement de production, il est important de protéger la base de données et de faire des sauvegardes régulièrement.

Nous utiliserons la version *bundle* de MySQL. Elle devrait contenir toutes les fonctions requises pour cette configuration minimale. Si vous souhaitez personnaliser la base de données selon vos préférences, vous devrez compiler MySQL depuis ses sources.

### 4.4.1 Installation de MySQL

En tant que `ejbca`, exécuter la commande suivante :

```
ejbca@server:~$ sudo apt-get install mysql-server mysql-client
```

### 4.4.2 Démarrage automatique de MySQL

Si l'instance n'est pas lancée, lancez MySQL à l'aide de la commande suivante :

```
ejbca@server:~$ sudo /etc/init.d/mysql start
```

### 4.4.3 Vérification de l'installation de MySQL

Pour vérifier que l'installation de MySQL est correcte, vous devez être capable de faire :

```
ejbca@server:~$ mysql mysql -u root -p
```

Puis, vous pouvez voir les utilisateurs par défaut du système :

```
mysql> select * from user;
| Host | User | Password | Select_priv | Insert_priv | Update_priv | Delete_priv |
Create_priv | Drop_priv | Reload_priv | Shutdown_priv | Process_priv | File_priv |
Grant_priv | References_priv | Index_priv | Alter_priv | Show_db_priv | Super_priv |
Create_tmp_table_priv | Lock_tables_priv | Execute_priv | Repl_slave_priv |
Repl_client_priv | Create_view_priv | Show_view_priv | Create_routine_priv |
Alter_routine_priv | Create_user_priv | ssl_type | ssl_cipher | x509_issuer |
x509_subject | max_questions | max_updates | max_connections | max_user_connections |
```

```
| localhost | root | | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | | | | 0 | 0 | 0 | 0 |
| server.edu.ejbca.org | root | | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | | | | 0 | 0 | 0 | 0 |
| server.edu.ejbca.org | | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| N | N | N | N | N | N | N | N | N | N | | | | 0 | 0 | 0 | 0 |
| localhost | | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
N | N | N | N | N | N | N | N | | | | 0 | 0 | 0 | 0 |
```

## 4.5 Installation de Java et JCE

Télécharger Java depuis : <http://java.sun.com/javase/downloads/>

Rubrique : Java SE Development Kit > JDK 6 Update <NN>.

```
ejbca@server:~$ cd /opt/sources
ejbca@server:/opt/sources$ wget <LIENS-VERS-LE-FICHER-AUTO-EXTRACTIBLE>
```

Puis exécutez le fichier binaire (**bin**) qui est un fichier auto-extractible. Ce dernier décompressera son contenu dans le répertoire courant (vérifiez avec la commande « **pwd** ») :

```
ejbca@server:/opt/sources$ cd /opt/tools
ejbca@server:/opt/tools$ cp /opt/sources/jdk-6u<NN>-linux-i586.bin .
ejbca@server:/opt/tools$ pwd
/opt/tools
ejbca@server:/opt/tools$ sh jdk-6u<NN>-linux-i586.bin
```

Faite un lien symbolique pour Java :

```
ejbca@server:/opt/tools$ ln -s jdk1.6.0_<NN>/ java
```

Pour autoriser Java à générer des clés de grande taille (plus que 1024 bits), nous avons besoin de télécharger l'extension « **Java Cryptography Extension** » (**JCE**) depuis l'adresse suivante : <http://java.sun.com/javase/downloads/>. Allez à la rubrique : *Additional ressources* > *Other Downloads* > *Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6*. Puis cliquez sur le bouton « Download ».

Décompressez les fichiers du JCE, puis déplacez les dans le répertoire « **lib/security** » du JRE (Java Runtime Environment) :

```
ejbca@server:/opt/tools$ cd /opt/sources/
ejbca@server:/opt/sources$ unzip jce_policy-6.zip
ejbca@server:/opt/sources$ mv jce/* /opt/tools/java/jre/lib/security/
ejbca@server:/opt/sources$ rmdir /opt/sources/jce/
```

Vous devriez avoir les fichiers et les répertoires suivants pour Java :

```
ejbca@server:/opt/sources$ cd /opt/tools
ejbca@server:/opt/tools$ ls -l /opt/tools/java/
drwxr-xr-x  2 ejbca ejbca   4096 2009-05-21 13:26 bin
-r--r--r--  1 ejbca ejbca   3767 2009-05-21 11:24 COPYRIGHT
drwxr-xr-x  7 ejbca ejbca   4096 2009-05-21 13:26 db
drwxr-xr-x 10 ejbca ejbca   4096 2009-05-21 13:26 demo
drwxr-xr-x  3 ejbca ejbca   4096 2009-05-21 13:26 include
drwxr-xr-x  7 ejbca ejbca   4096 2009-06-24 11:09 jre
drwxr-xr-x  3 ejbca ejbca   4096 2009-06-24 11:09 lib
```

```

-r--r--r-- 1 ejbca ejbca 17064 2009-05-21 11:24 LICENSE
drwxr-xr-x 4 ejbca ejbca 4096 2009-05-21 13:26 man
-r--r--r-- 1 ejbca ejbca 28329 2009-05-21 11:24 README.html
-r--r--r-- 1 ejbca ejbca 25390 2009-05-21 11:24 README_ja.html
-r--r--r-- 1 ejbca ejbca 20768 2009-05-21 11:24 README_zh_CN.html
-r--r--r-- 1 ejbca ejbca 5190 2009-06-24 11:09 register.html
-r--r--r-- 1 ejbca ejbca 5622 2009-06-24 11:09 register_ja.html
-r--r--r-- 1 ejbca ejbca 4800 2009-06-24 11:09 register_zh_CN.html
drwxr-xr-x 9 ejbca ejbca 4096 2009-05-21 13:26 sample
-rw-r--r-- 1 ejbca ejbca 19026975 2009-05-21 11:24 src.zip
-r--r--r-- 1 ejbca ejbca 249556 2009-05-21 11:24 THIRDPARTYLICENSEREADME.txt

```

... et les fichiers suivants pour JCE :

```

ejbca@server:/opt/tools$ ls -l /opt/tools/java/jre/lib/security/
-r--r--r-- 1 ejbca ejbca 68595 2009-05-21 11:06 cacerts
-r--r--r-- 1 ejbca ejbca 2663 2006-11-17 03:10 COPYRIGHT.html
-r--r--r-- 1 ejbca ejbca 2221 2009-05-21 11:06 java.policy
-r--r--r-- 1 ejbca ejbca 9937 2009-05-21 11:06 java.security
-r--r--r-- 1 ejbca ejbca 132 2009-05-21 11:28 javaws.policy
-rw-r--r-- 1 ejbca ejbca 2481 2006-11-17 03:10 local_policy.jar
-r--r--r-- 1 ejbca ejbca 8386 2006-11-17 03:10 README.txt
-rw-r--r-- 1 ejbca ejbca 2465 2006-11-17 03:10 US_export_policy.jar

```

## 4.6 Installation du serveur d'applications

### 4.6.1 Installation de JBoss

Téléchargez le serveur d'applications JBoss depuis l'adresse suivante :

<http://labs.jboss.com/portal/jbossas/download>

Et sélectionnez « *download* » pour télécharger la version <VERSION-JBOSS>.

En tant que `root`, allez dans le répertoire d'installation `/opt/sources` et décompressez JBoss :

```

ejbca@server:~$ cd /opt/sources/
ejbca@server:/opt/sources/$ unzip /opt/sources/jboss-<VERSION-JBOSS>.GA.zip
ejbca@server:/opt/sources/$ mv /opt/sources/jboss-<VERSION-JBOSS>.GA /opt/tools/

```

Faites un lien symbolique vers le répertoire `jboss-<VERSION-JBOSS>` et nommez le `jboss` :

```

ejbca@server:/opt/sources/$ cd /opt/tools/
ejbca@server:/opt/tools/$ ln -s jboss-<VERSION-JBOSS>.GA/ jboss

```

Vous devriez avoir les fichiers et les répertoires suivants :

```

ejbca@server:/opt/tools/$ ls -l /opt/tools/jboss/
drwxr-xr-x 2 ejbca ejbca 4096 2009-05-22 16:23 bin
drwxr-xr-x 2 ejbca ejbca 4096 2009-05-22 11:03 client
drwxr-xr-x 3 ejbca ejbca 4096 2009-05-22 11:01 common
-rw-r--r-- 1 ejbca ejbca 6133 2009-05-22 16:19 copyright.txt
drwxr-xr-x 7 ejbca ejbca 4096 2009-05-22 16:19 docs
-rw-r--r-- 1 ejbca ejbca 107376 2009-05-22 11:04 jar-versions.xml
-rw-r--r-- 1 ejbca ejbca 8074 2009-05-22 16:19 JBossORG-EULA.txt
-rw-r--r-- 1 ejbca ejbca 33732 2009-05-22 16:19 lgpl.html
drwxr-xr-x 3 ejbca ejbca 4096 2009-05-22 11:04 lib

```

```
-rw-r--r-- 1 ejbca ejbca 36365 2009-05-22 16:19 readme.html
drwxr-xr-x 7 ejbca ejbca 4096 2009-05-22 11:02 server
```

## 4.7 Installation de Ant

Ant est comme « make » mais pour Java. Cela signifie que Ant exécute plusieurs commandes selon un fichier de contrôle « `build.xml` » dépendant de la cible voulue par l'utilisateur.

Téléchargez Ant depuis l'adresse suivante :

<http://ant.apache.org/bindownload.cgi>

... puis sélectionnez le fichier `apache-ant-<VERSION-ANT>-bin.tar.bz2` :

```
ejbca@server:~$ cd /opt/sources/
ejbca@server:/opt/sources/$ tar jxvf /opt/sources/apache-ant-<VERSION-ANT>-bin.tar.bz2
ejbca@server:/opt/sources/$ mv apache-ant-<VERSION-ANT> /opt/tools/
ejbca@server:/opt/sources/$ cd /opt/tools/
```

Puis ajoutez le lien symbolique suivant, pour définir le chemin général de recherche de Ant :

```
ejbca@server:/opt/sources/$ cd /opt/tools/
ejbca@server:/opt/tools/$ ln -s apache-ant-<VERSION-ANT>/ ant
```

Vous devriez avoir les fichiers et les répertoires suivants :

```
ejbca@server:/opt/tools/$ ls -l /opt/tools/ant/
drwxr-xr-x 2 ejbca ejbca 4096 2009-06-24 10:29 bin
drwxr-xr-x 9 ejbca ejbca 4096 2009-06-24 10:29 docs
drwxr-xr-x 3 ejbca ejbca 4096 2009-06-24 10:29 etc
-rw-r--r-- 1 ejbca ejbca 7160 2008-06-27 07:04 fetch.xml
-rw-r--r-- 1 ejbca ejbca 4445 2008-06-27 07:04 get-m2.xml
-rw-r--r-- 1 ejbca ejbca 126 2008-06-27 07:04 INSTALL
-rw-r--r-- 1 ejbca ejbca 51380 2008-06-27 07:04 KEYS
drwxr-xr-x 2 ejbca ejbca 4096 2009-06-24 10:29 lib
-rw-r--r-- 1 ejbca ejbca 15289 2008-06-27 07:04 LICENSE
-rw-r--r-- 1 ejbca ejbca 1270 2008-06-27 07:04 NOTICE
-rw-r--r-- 1 ejbca ejbca 4119 2008-06-27 07:04 README
-rw-r--r-- 1 ejbca ejbca 146814 2008-06-27 07:04 WHATSNEW
```

## 4.8 Installations spécifiques

### 4.8.1 Installation du pilote MySQL pour JBoss

Cette partie permet au serveur d'applications de se connecter à la base de données. Ainsi, si vous choisissez une autre base de données que MySQL, il vous aurez besoin d'un autre connecteur.

Téléchargez le connecteur MySQL Java depuis l'adresse suivante :

<http://dev.mysql.com/downloads/connector/j/>

Décompressez et déplacez le connecteur dans le répertoire `server/default/lib` de JBoss :

```
ejbca@server:~$ cd /opt/sources
```

```
ejbca@server:/opt/sources/$ tar zxvf /opt/sources/mysql-connector-java-5.1.7.tar.gz
ejbca@server:/opt/sources/$ cp /opt/sources/mysql-connector-java-5.1.7/mysql-
connector-java-5.1.7-bin.jar /opt/tools/jboss/server/default/lib/
```

Vérifiez que vous avez bien le fichier suivant :

```
ejbca@server:~$ cd /opt/tools
ejbca@server:/opt/tools/$ ls -l jboss/server/default/lib/mysql-connector-java-*
-rw-r--r-- 1.ejbca.ejbca.709922.2009-06-24.15:42.jboss/server/default/lib/mysql-
connector-java-5.1.7-bin.jar
```

## 4.9 Installation de l'application EJBCA

Téléchargez EJBCA depuis : <http://www.ejbca.org/>

... puis, sélectionnez « *download* » et téléchargez la dernière version.

En tant que **root**, décompressez EJBCA dans le répertoire **/usr/local** :

```
ejbca@server:~$ cd /opt/sources/
ejbca@server:/opt/sources/$ unzip /opt/sources/ejbca_3_9_0.zip
ejbca@server:/opt/sources/$ mv.ejbca_3_9_0/opt/tools
ejbca@server:/opt/sources/$ cd /opt/tools
ejbca@server:/opt/tools/$ ln -s.ejbca_3_9_0/.ejbca
```

Vous devriez avoir les fichiers et les répertoires suivants :

```
ejbca@server:~$ ls -l /opt/tools/ejbca/
-rw----- 1.ejbca.ejbca.2640.2009-06-05.09:26.avk.xml
drwx----- 3.ejbca.ejbca.4096.2009-06-05.09:34.bin
-rw----- 1.ejbca.ejbca.49969.2009-06-05.09:26.build.xml
-rw----- 1.ejbca.ejbca.87923.2009-06-05.09:26.Changelog.txt
drwx----- 2.ejbca.ejbca.4096.2009-06-05.09:23.cloverdata
-rw----- 1.ejbca.ejbca.4384.2009-06-05.09:24.cmptcp.xml
-rw----- 1.ejbca.ejbca.39873.2009-06-05.09:24.compile.xml
drwx----- 3.ejbca.ejbca.4096.2009-06-05.09:34.conf
drwx----- 8.ejbca.ejbca.4096.2009-06-05.09:24.doc
-rw----- 1.ejbca.ejbca.3843.2009-06-05.09:24.docs.xml
-rw----- 1.ejbca.ejbca.1435.2009-06-05.09:26.externalra.xml
-rw----- 1.ejbca.ejbca.13467.2009-06-05.09:24.jaxws.xml
drwx----- 12.ejbca.ejbca.4096.2009-06-05.09:26.lib
-rw----- 1.ejbca.ejbca.20290.2009-06-05.09:34.propertiesAndPaths.xml
-rw----- 1.ejbca.ejbca.139.2009-06-05.09:24.README
drwx----- 16.ejbca.ejbca.4096.2009-06-05.09:24.src
-rw----- 1.ejbca.ejbca.21759.2009-06-05.09:23.test.xml
-rw----- 1.ejbca.ejbca.8807.2009-06-05.09:24.xkms.xml
```

## 5 Configuration d'EJBCA

Dans ce chapitre, nous allons finir l'installation afin d'aboutir à une application EJBCA fonctionnelle. Nous allons configurer et interconnecter toutes les parties dont la plate-forme EJBCA a besoin.

### 5.1 Variables d'environnement

Les variables d'environnement permettent à chaque partie de savoir où sont les autres.

Éditez le fichier `/home/ejbca/.profile` en ajoutant les lignes suivantes :

```
JBOSS_HOME=/opt/tools/jboss
APPSRV_HOME=/opt/tools/jboss
JAVA_HOME=/opt/tools/java
JAVA_OPTS="-Xmx512M -Xms512M"
EJBCA_HOME=/opt/tools/ejbca
ANT_HOME=/opt/tools/ant

PATH=${JBOSS_HOME}/bin:${APPSRV_HOME}/bin:${JAVA_HOME}/bin:${EJBCA_HOME}/bin:${
ANT_HOME}/bin:$PATH

export PATH JBOSS_HOME APPSRV_HOME JAVA_HOME JAVA_OPTS EJBCA_HOME ANT_HOME
```

Déconnectez vous, puis connectez vous à nouveau.

Vérifiez que les variables d'environnement sont bien positionnées

```
ejbca@server:/opt/tools/ejbca$ env | egrep 'JAVA_HOME|JAVA_OPTS|EJBCA_HOME|ANT_HOME|
JBOSS_HOME'
JBOSS_HOME=/opt/tools/jboss
ANT_HOME=/opt/tools/ant
EJBCA_HOME=/opt/tools/ejbca
JAVA_OPTS="-Xmx512M -Xms512M"
JAVA_HOME=/opt/tools/java
```

**Remarque :** si les variables n'apparaissent pas au cours du test, vous devez exécuter la commande suivante : « `ejbca@server:/opt/tools/ejbca$ source /etc/profile` ».

### 5.2 Création de la base de données et du compte « ejbca »

#### 5.2.1 Création de la base de données MySQL

Maintenant, nous allons créer la base de données dans laquelle toutes les données seront stockées.

En tant que `root`, créez la base de données MySQL :

```
ejbca@server:~$ mysqladmin create -u root -p ejbca3
Password: [appuyez seulement sur la touche "Entrée"]
```



```
ejbca@server:/opt/tools/ejbca/conf$ cp ejbca.properties.sample ejbca.properties
```

Nous allons maintenant adapter ce fichier de configuration.

Éditez le fichier « `ejbca.properties` » et modifiez les propriétés suivantes.

Nom de l'administrateur de l'AC « AdminCA1 » :

```
ca.name=AdminCA1
ca.dn=CN=AdminCA1,O=EJBCA Sample,C=FR
```

Changez la taille et le type de clés des AC :

```
ca.keyspec=4096
ca.keytype=RSA
```

En environnement de **production**, la taille d'une clé d'AC doit être de **4096 bits**.

Positionnez l'algorithme de signature sur le couple RSA/SHA-1 :

```
ca.signaturealgorithm=SHA1withRSA
```

Positionnez la durée de validité à 365 jours :

```
ca.validity=365
```

Vérifiez que la valeur de la politique est positionnée à « `null` ». Dans un environnement de production, ce champ doit contenir l'OID d'une politique de certification réelle.

```
ca.policy=null
```

Choisir un mot de passe complexe pour l'AC. Ce mot de passe sera utilisé pour toutes les AC sur support logiciel.

Comme il n'est pas nécessaire de mémoriser ce mot de passe, il peut être très complexe.

```
ca.keystorepass=aYRf142Dg
```

### 5.3.2 Fichier « `database.properties` »

Copiez l'échantillon du fichier de configuration « `database.properties` » :

```
ejbca@server:/opt/tools/ejbca/conf$ cp database.properties.sample database.properties
```

Nous allons maintenant adapter ce fichier de configuration.

Éditez le fichier « `database.properties` » et modifiez les propriétés suivantes.

Positionnez les paramètres suivants pour la base de données MySQL :

```
database.name=mysql
datasource.mapping=mysql
```

Paramétrage du nom de l'hôte, du numéro de port et le nom de la base de données (qui a été précédemment créée) :

```
database.url=jdbc:mysql://127.0.0.1:3306/ejbca3
```

**Ne pas oublier** le chiffre « 3 » à la fin du champ « `database.url` » afin de correctement désigner le nom de la base de données.

Ce paramètre positionne le nom de la classe du connecteur de la base de données (que nous avons copié dans le répertoire « `lib` » de JBoss, précédemment).

```
database.driver=com.mysql.jdbc.Driver
```

Indiquez à EJBCA l'identifiant et le mot de passe du compte se connectant à la base :

```
database.username=ejbca3  
database.password=ejbcapass
```

### 5.3.3 Fichier « `web.properties` »

Copiez l'échantillon du fichier de configuration « `web.properties` » :

```
ejbca@server:/opt/tools/ejbca/conf$ cp web.properties.sample web.properties
```

Nous allons maintenant adapter ce fichier de configuration.

Paramétrage du mot de passe pour le magasin des AC de confiance « `cacerts` »

```
java.trustpassword=changeit
```

**Remarque :** le magasin « `cacerts` » existe dès l'installation de Java, car il contient les AC de confiance utilisées par Tomcat pour faire de l'authentification client.

Le mot de passe du `superadmin` devrait être un bon mot de passe, car il fournit tous les accès possibles. Vous aurez besoin de ce mot de passe plus tard lorsque vous importerez le certificat du `superadmin` dans votre navigateur web.

```
superadmin.password=ejbca
```

Définissez le mot de passe utilisé pour le magasin `keystore` du serveur HTTPS. Ce mot de passe doit être complexe.

```
httpserver.password=lkjrdgSDE3
```

Définissez le nom (DN) du certificat utilisé par le serveur web de JBoss, ainsi que son nom de domaine complet (FQDN). L'attribut CN contient le nom de domaine complet du serveur web.

```
httpserver.hostname=localhost  
httpserver.dn=CN=${httpserver.hostname},O=EJBCA Sample,C=FR
```

Il est **très important** que le champ « `httpserver.hostname` » et l'attribut CN du champ « `httpserver.dn` » aient la même valeur, pour éviter toute confusion.

### 5.3.4 Autres fichiers de propriétés

Les autres fichiers de configuration sont gardés tels quels pour ce cours.

## 5.4 Démarrage d'EJBCA

### 5.4.1 Arrêt du serveur d'applications JBoss

Avant de continuer, veuillez arrêter le serveur JBoss :

```
ejbca@server:~$ ps -ef | grep java
```

Il ne devrait pas avoir de message en retour. Mais si c'est le cas, alors vous devriez obtenir un message similaire à celui-ci :

```
ejbca      3197   3179  56 05:37 pts/0      00:00:51 /opt/tools/java/bin/java
-Dprogram.name=run.sh -server -Xms128m -Xmx512m
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000
-Djava.endorsed.dirs=/opt/tools/jboss/lib/endorsed -classpath
/opt/tools/jboss/bin/run.jar:/opt/tools/java/lib/tools.jar org.jboss.Main
```

Si JBoss tourne, veuillez presser Ctrl+C dans la console dans laquelle il a été lancé :

```
ejbca@server:~$ cd /opt/tools/jboss
ejbca@server:/opt/tools/jboss$ ./bin/shutdown.sh -S
```

### 5.4.2 Changement de propriétaires des fichiers installés

Comme JBoss va être lancé en tant qu'utilisateur et non en tant que `root` (ce qui est fortement déconseillé), tous les fichiers devront être accessibles par l'utilisateur `ejbca` :

```
ejbca@server:~$ cd /opt/tools/
ejbca@server:/opt/tools/$ chown -R ejbca ejbca/
ejbca@server:/opt/tools/$ chown -R ejbca jboss/
```

**Attention : n'oublier pas le slash « / » à la fin du nom du répertoire.** Sinon, vous ne changerez que les droits du lien et non de toute l'arborescence du répertoire pointé.

**Remarque :** à partir de maintenant, l'usage de l'utilisateur `root` est restreint et, sans précision, vous n'utiliserez que le compte `ejbca`.

Depuis que JBoss tourne en tant que `ejbca`, il ne pourra plus lire ni écrire les fichiers créés et/ou édités en tant que `root`. Donc, en cas de problème, pensez à vérifier les droits de vos fichiers, cela vous fera gagner du temps pour trouver la cause de l'erreur.

### 5.4.3 Initialisation d'EJBCA : tâche « Bootstrap »

À cette étape, nous allons compiler tous les fichiers sources et *packager* les exécutables et la configuration dans un fichier EAR (*i.e.* une sorte de fichier Zip avec une structure standardisée) qui sera copié dans le répertoire `jboss` de l'application.

```
ejbca@server:~$ cd /opt/tools/ejbca
ejbca@server:/opt/tools/ejbca$ ant bootstrap
```

Vérifiez que tous les fichiers sont installés dans le répertoire `jboss` :

```
ejbca@server:/opt/tools/ejbca$ ls -l /opt/tools/jboss/server/default/deploy/ejbca*
-rw----- 1 ejbca ejbca      2721 2009-06-24 16:44
../jboss/server/default/deploy/ejbca-ds.xml
```

```
-rw-r--r-- 1 ejbca ejbca 45482792 2009-06-24 16:44
../jboss/server/default/deploy/ejbca.ear
-rw----- 1 ejbca ejbca      1919 2009-06-24 16:44
../jboss/server/default/deploy/ejbca-mail-service.xml
```

Consultez les journaux de Ant après son déploiement.

### 5.4.4 Démarrage du serveur d'applications JBoss

Maintenant nous allons démarrer l'application EJBCA pour la première fois. Puis au cours de ce chapitre, nous verrons comment créer notre première AC et le compte du `superadmin`.

```
ejbca@server:~$ cd /opt/tools/jboss
ejbca@server:/opt/tools/jboss$ ./bin/run.sh
```

Vérifiez les lignes suivantes :

```
22:55:35,879 INFO [EARDeployer] Init J2EE application: file:/opt/tools/jboss-<VERSION-
JBOSS>.GA/server/default/deploy/ejbca.ear
22:55:54,067 INFO [EjbModule] Deploying PublisherData
22:55:54,858 INFO [EjbModule] Deploying CertReqHistoryData
[lots of rows like that]
22:56:17,975 INFO [BaseLocalProxyFactory] Bound EJB LocalHome 'PublisherData' to jndi
'PublisherDataLocal'
[lots of rows like that]
22:56:23,282 INFO [EJBDeployer] Deployed: file:/opt/tools/jboss-<VERSION-
JBOSS>.GA/server/default/tmp/deploy/tmp10234ejbca.ear-contents/ejbca-ejb.jar
22:56:34,218 INFO [StartServicesServlet] Init, EJBCA startup.
22:57:19,925 INFO [EARDeployer] Started J2EE application: file:/opt/tools/jboss-
<VERSION-JBOSS>.GA/server/default/deploy/ejbca.ear
```

... jusqu'à voir une ligne similaire à la suivante :

```
21:09:03,488 INFO [Server] JBoss (MX MicroKernel) [<VERSION-JBOSS>.GA (build:
CVSTag=Branch_4_0 date=200610162339)] Started in 1m:22s:389ms
```

Désormais le serveur JBoss a démarré avec la configuration initiale de EJBCA.

Mais si vous recevez les lignes suivantes :

```
Last packet sent to the server was 13 ms ago.); - nested throwable:
(org.jboss.resource.JBossResourceException: Could not create connection; -
nested throwable: (com.mysql.jdbc.CommunicationsException: Communications link failure
due to underlying exception:

java.net . ConnectionException
MESSAGE: Connection Refused
```

... cela signifie que la base de données MySQL n'a pas démarré.

Vérifiez que la base de données a été peuplée.

Vérifiez que vous pouvez vous connecter à la nouvelle base avec le nouveau utilisateur :

```
mysql ejbca3 -u ejbca3 -p
mysql> show tables;
+-----+
| Tables_in_ejbca3 |
```

```
+-----+
| AccessRulesData |
| AdminEntityData |
| AdminGroupData |
| AdminPreferencesData |
| ApprovalData |
| AuthorizationTreeUpdateData |
| CAData |
| CRLData |
| CertReqHistoryData |
| CertificateData |
| CertificateProfileData |
| EndEntityProfileData |
| GlobalConfigurationData |
| HardTokenCertificateMap |
| HardTokenData |
| HardTokenIssuerData |
| HardTokenProfileData |
| HardTokenPropertyData |
| KeyRecoveryData |
| LogConfigurationData |
| LogEntryData |
| PublisherData |
| ServiceData |
| TableProtectData |
| UserData |
| UserDataSourceData |
+-----+
26 rows in set (0.00 sec)
```

**Attention :** si vous n’avez pas de table dans votre base de données MySQL, **arrêtez ce processus**. Cette étape « bootstrap » doit être exécutée avec succès, pour pouvoir continuer.

### 5.4.5 Installation d’EJBCA

À cette étape, nous allons créer la première AC avec le compte du superadmin.

**Attention :** veuillez vérifier qu’à partir de cette étape la date et l’heure sont correctement réglées sur le serveur des AC.

Ouvrez une console sur le serveur et lancez la commande d’installation :

```
ejbca@server:~$ cd /opt/tools/ejbca
ejbca@server:/opt/tools/ejbca$ ant install
```

Vous devriez voir des entrées de journal JBoss similaires à celles-ci :

```
23:01:50,416 INFO [Log4jLogDevice] 21 March 2007 23:01:50 CET, CAId : -2095769233, RA,
EVENT_INFO_EDITEDADMINISTRATORPRIVILEGES, Administrator : CACMDLINE, User : No user
involved, Certificate : No certificate involved, Comment : Administratorgroup Temporary
Super Administrator Group added.
23:01:51,101 INFO [Log4jLogDevice] 21 March 2007 23:01:50 CET, CAId : -2095769233, RA,
EVENT_INFO_EDITEDADMINISTRATORPRIVILEGES, Administrator : CACMDLINE, User : No user
involved, Certificate : No certificate involved, Comment : Added administrator entities
to administratorgroup Temporary Super Administrator Group.
23:01:51,161 INFO [Log4jLogDevice] 21 March 2007 23:01:51 CET, CAId : -2095769233, RA,
EVENT_INFO_EDITEDADMINISTRATORPRIVILEGES, Administrator : CACMDLINE, User : No user
```

```
involved, Certificate : No certificate involved, Comment : Added accessrules to  
admingroup Temporary Super Administrator Group.
```

**Remarque :** vous pouvez ignorer l'erreur suivante, car nous traiterons ce problème dans le prochain chapitre.

```
[exec] keytool error: java.io.FileNotFoundException: /opt/tools/jdk1.5.0_<NN>/jre/lib/  
security/cacerts (Permission denied)
```

#### 5.4.6 Initialisation du magasin de clés « javastruststore »

Cette étape donnée à titre d'information est facultative, **veuillez passer à l'étape suivante.**

Le certificat de l'AC récemment générée doit être inséré dans le magasin Java « truststore ». Pour cela JBoss doit être capable de communiquer en SSL avec le certificat superadmin (qui est émis par la nouvelle AC).

Lorsque vous faite une installation Ant en tant qu'utilisateur hors système, vous n'avez pas la permission d'écriture dans le *truststore* Java. La meilleure façon de résoudre ce problème est de relancer l'étape d'insertion en tant que *root* (en utilisant *sudo*).

Ainsi, la commande Ant doit être exécutée en tant que *root* à travers l'outil *sudo*.

```
ejbca@server:~$ cd /opt/tools/ejbca
```

Indiquez à EJBCA d'insérer le certificat de l'AC récemment générée dans le *truststore* Java :

```
ejbca@server:/opt/tools/ejbca$ sudo ant javatruststore  
Buildfile: build.xml  
  
javatruststore:  
  
ejbca:javatruststore:  
[echo] Creating root certificate in DER format...  
[echo] ca getrootcert EjbcaCourseCA1 /tmp/rootca.der -der  
[java] Wrote Root CA certificate to '/tmp/rootca.der'  
[exec] keytool error: java.lang.Exception: Alias <EJBCA-CA> does not exist  
[exec] Result: 1  
[exec] [Storing /opt/tools/jdk1.5.0_<NN>/jre/lib/security/cacerts]  
[exec] Certificate was added to keystore  
[exec] [Storing /opt/tools/jdk1.5.0_<NN>/jre/lib/security/cacerts]  
[delete] Deleting: /tmp/rootca.der  
  
BUILD SUCCESSFUL  
Total time: 5 seconds
```

**Remarque :** toute référence au message « *Alias ... does not exist* » peut être ignorée en toute sécurité. Cela signifie simplement qu'il s'agit de la première installation de ce nom d'AC.

Vérifiez le magasin Java « *truststore* » avec la commande suivante :

```
server:/opt/tools/ejbca$ keytool -list -keystore  
/opt/tools/java/jre/lib/security/cacerts  
[...]  
adminca1, 21-Mar-2007, trustedCertEntry,  
Certificate fingerprint (MD5): 87:9D:A8:B2:D4:9C:1C:AD:BB:F6:0E:EF:A0:18:13:3D
```

Le mot de passe par défaut est « **changeit** ».

Comme vous pouvez le constater, il existe déjà un grand nombre d'AC fournies avec Java.

Dans un environnement de production, vous devriez supprimer le fichier **cacerts** avant d'exécuter la commande « **ant javatruststore** ». Ainsi, EJBCA en créera un nouveau avec une seule entrée contenant la nouvelle AC.

Un fichier **cacerts** minimal évite que les entités émises par les AC incluses dans le fichier **cacerts** puissent être capables de s'authentifier via une connexion SSL à l'AC installée. Il existe plusieurs raisons pour protéger ce qu'un client peut faire, mais aucune raison pour ne pas nettoyer ce fichier.

### 5.4.7 Arrêt du serveur d'applications JBoss

Avant de continuer, il est préférable d'arrêter le serveur JBoss afin qu'il puisse prendre en compte les changements nécessaires pour l'étape suivante.

```
ejbca@server:~$ ps -ef | grep jboss
ejbca      7405   7386   1 12:21 pts/3      00:01:14 /opt/tools/java/bin/java
-Dprogram.name=run.sh -server -Xmx512M -Xms512M -Djava.net.preferIPv4Stack=true
-Djava.endorsed.dirs=/opt/tools/jboss/lib/endorsed -classpath
/opt/tools/jboss/bin/run.jar:/opt/tools/java/lib/tools.jar org.jboss.Main
```

Si vous constatez que JBoss tourne, veuillez presser Ctrl+C dans la console où le serveur a été démarré :

```
ejbca@server:~$ cd /opt/tools/jboss
ejbca@server:/opt/tools/jboss$ ./bin/shutdown.sh -S

Wait for:
23:05:30,641 INFO [Server] Shutdown complete
Shutdown complete
```

### 5.4.8 Déploiement d'EJBCA

À cette étape, nous allons configurer JBoss avec un certificat (fichier **tomcat.jks**). La mise à jour du **cacerts** et la configuration des ports se font avec la commande « **ant deploy** ». Ainsi Ant applique ces changements à JBoss via le fichier « **build.xml** »

Exécutez Ant pour l'étape cible « **deploy** » :

```
ejbca@server:/opt/tools/ejbca$ ant deploy
```

Vérifiez la présence du **keystore** pour Tomcat (le *frontend* web de JBoss) :

```
ejbca@server:/opt/tools/ejbca$ ls -l /opt/tools/jboss/server/default/conf/keystore/
-rw----- 1 ejbca users 2672 2007-03-21 23:06 keystore.jks
```

### 5.4.9 Démarrage du serveur d'applications JBoss

Désormais, tous les éléments devraient être en place pour notre serveur que nous devons démarrer à nouveau :

```
ejbca@server:/opt/tools/jboss$ ./bin/run.sh
```

Vérifiez dans les journaux que les ports 8080, 8442 et 8443 sont liés à JBoss :

```
23:09:04,128 INFO [EARDeployer] Started J2EE application: file:/opt/tools/jboss-
<VERSION-JBOSS>.GA/server/default/deploy/ejbca.ear
23:09:04,272 INFO [Http11BaseProtocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-8080
23:09:04,522 INFO [ChannelSocket] JK: ajp13 listening on /0.0.0.0:8009
23:09:04,644 INFO [JkMain] Jk running ID=0 time=0/156 config=null
23:09:04,709 INFO [Http11BaseProtocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-8442
23:09:04,783 INFO [Http11BaseProtocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-8443
```

Attendez de voir apparaître l'entrée de journal suivante :

```
23:09:04,800 INFO [Server] JBoss (MX MicroKernel) [<VERSION-JBOSS>.GA (build:
CVSTag=Branch_4_0 date=200610162339)] Started in 1m:56s:517ms
```

Vérifiez que la base de données a été peuplée :

```
ejbca@server:/opt/tools/ejbca$ mysql ejbca3 -u ejbca3 -p
mysql> select * from AdminEntityData;
+-----+-----+-----+-----+-----+-----+
| pK | matchWith | matchType | matchValue | AdminGroupData_adminEntities |
+-----+-----+-----+-----+-----+
| -794119294 | 8 | 1001 | SuperAdmin | 992914344 |
| 329358383 | 11 | 2003 | UNUSED | -2073580008 |
| 329358381 | 11 | 2001 | UNUSED | -2073580008 |
| 329358382 | 11 | 2002 | UNUSED | -2073580008 |
| 329358376 | 11 | 2004 | UNUSED | -2073580008 |
| -752132537 | 11 | 2000 | UNUSED | 1030885333 |
+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)
```

## 5.5 Démarrage de la console d'administration web

### 5.5.1 Importation du certificat « SuperAdmin » dans un navigateur

Pour pouvoir administrer EJBCA, vous devez avoir le certificat du superadmin installé dans votre navigateur à partir d'un fichier au format PKCS #12 protégé avec le mot de passe défini dans le fichier de configuration d'EJBCA.

Copiez le fichier suivant sur votre poste de travail :

```
/opt/tools/ejbca/p12/superadmin.p12
```

Puis, importez le fichier PKCS #12 dans votre navigateur web (e.g. Firefox, Opera, Safari, IE).

### 5.5.2 Démarrage de l'administration web d'EJBCA

Allez sur l'interface web d'administration d'EJBCA :

```
https://localhost:8443/ejbca/adminweb/
```

## 6 Initialisation de l'IGC

### 6.1 Service de publication LDAP

Afin de terminer l'installation et avant de procéder à la cérémonie de clés, il est nécessaire de configurer le service de publication pour publier les nouveaux certificats et LCR vers l'annuaire LDAP.

#### 6.1.1 Création du service de publication

Pour créer un nouveau service de publication, il faut sélectionner le menu « Services de publication » et ajouter un nom dans le champ prévu à cet effet.

Un appui sur le bouton « Ajouter » permet d'ajouter un nouvel identifiant de service de publication dans la liste des services de publication.

L'identifiant du service de publication LDAP peut être nommé de la façon suivante :

```
PS_<NOM-ENTREPRISE>
```

#### 6.1.2 Édition du service de publication

Une fois le nouvel identifiant du service de publication créé, il est nécessaire de configurer le service de publication pour le faire communiquer avec l'annuaire LDAP. Pour ce faire, veuillez sélectionner le nom précédemment créé et appuyer sur le bouton « Éditer service de publication ».

Une fois cette action réalisée, une page permettant de configurer le service de publication apparaît dans l'interface.

La configuration du service de validation est réalisée par la saisie des différents champs et l'appui sur le bouton « Sauvegarder ». L'appui sur le bouton « Sauvegarder et tester connexion » permet de faire un appel à l'annuaire LDAP et de valider que l'accès soit autorisé.

### 6.2 Service de publication OCSP

La configuration d'un service de publication OCSP permet l'exportation de l'état des certificats dans une base de donnée externe qui sera utilisée par les répondeurs OCSP.

#### 6.2.1 Création du service de publication

Pour créer un nouveau service de publication, il faut sélectionner le menu « Services de publication » et ajouter un nom dans le champ prévu à cet effet.

Un appui sur le bouton « Ajouter » permet d'ajouter un nouvel identifiant de service de publication dans la liste des services de publication.

Dans le cadre de la PKI EJBCA, nous utiliserons l'identifiant `PS_OCSP` pour créer le service de publication OCSP.

## 6.2.2 Édition du service de publication

Une fois le nouvel identifiant du service de publication créé, il est nécessaire de configurer le service. Pour ce faire, vous devez sélectionner le nom précédemment créé et appuyer sur le bouton « Éditer service de publication ».

Une fois cette action réalisée, une page permettant de configurer le service de publication apparaît dans l'interface.

La configuration du service de validation est réalisée par la saisie des différents champs et l'appui sur le bouton « Sauvegarder ». L'appui sur le bouton « Sauvegarder et tester connexion » permet de faire un appel à la base de données et de valider que l'accès soit autorisé.

## 6.2.3 Création du profil de certificats OCSPSigner

Avant de procéder à la création des certificats utilisés pour signer les réponses OCSP, il convient de créer un profil de certificats basé sur OCSPSIGNER qui utilise le service de publication précédemment créé :

- cliquer sur le menu « Profil de certificats » ;
- sélectionner le profil « OCSPSIGNER (FIXED) » ;
- créer un nouveau service « OCSPSIGNER PUBLISHED » en utilisant le bouton « Utiliser le gabarit sélectionné » ;
- sélectionner le profil « OCSPSIGNER PUBLISHED » ;
- cliquer sur le bouton « Éditer un profil de certificats » ;
- sélectionner au minimum « `ps_ocsp` » comme services de publication.

Il conviendra d'utiliser ce service de publication pour chaque profil de certificats !

## 6.3 Validation et tests de bon fonctionnement

Pour être sûr que les fonctions principales d'EJBCA fonctionnent, nous allons émettre un certificat client et utiliser pour accéder à une page web protégée.

Comme maintenant nous commençons à faire une partie du cours « Administration d'EJBCA », nous allons seulement suivre les étapes sans chercher à les décrire.

### 6.3.1 Ajout d'un nouvel utilisateur

Allez à la rubrique : Administration > Fonctions d'AE > Ajouter une demande d'entité

**EJBCA Administration**

Accueil

**Ajouter une demande d'entité**

Fonctions d'AC  
 Fonctions de base  
 Activation d'AC  
 Profils de certificats  
 Services de publication  
 Editer/créer les AC

Fonctions d'AE  
 Gestion des données externes  
 Gestion des profils d'entités  
 Ajouter une demande d'entité  
 Lister/éditer les entités

Fonctions de supervision  
 Gestion des requêtes  
 Consulter les journaux  
 Configuration des journaux  
 Rapports

Fonctions système  
 Configuration du système  
 Gestion des services  
 Gestion des administrateurs  
 Mes préférences

Interface publique

Profil d'entités: **EMPTY**

Requis

Nom d'utilisateur

Mot de passe

Confirmation du mot de passe

Génération par lot

Courrier électronique  @

**Champs du DN du sujet**

emailAddress [E], Adresse de courriel (dans le DN) Utiliser les données depuis l'adresse de courriel :

UID, Identifiant unique

CN, Nom commun

serialNumber [SN], Numéro de série (dans le DN)

givenName, Prénom(s)

initials, Abréviations des prénoms

surname, Nom de famille

title [T], Titre

OU, Unité d'organisation

O, Organisation (raison sociale)

L, Ville

ST, État ou région

DC, Composante de domaine

C, Pays (ISO 3166)

Remplissez le formulaire avec au moins les champs et valeurs suivants :

Nom du champ	Valeur
Profil d'entités	EMPTY
Nom	test1
Mot de passe	foo123
Confirmer le mot de passe	foo123
CN, Nom commun	Test User
O, Organisation (raison sociale)	EJBCA Sample
C, Pays (ISO 3166)	FR
Profil de certificats	ENDUSER
AC	AdminCA1
Token	Généré par le navigateur

Puis, cliquer sur « Requête de certificat ».

### 6.3.2 Émission du certificat utilisateur

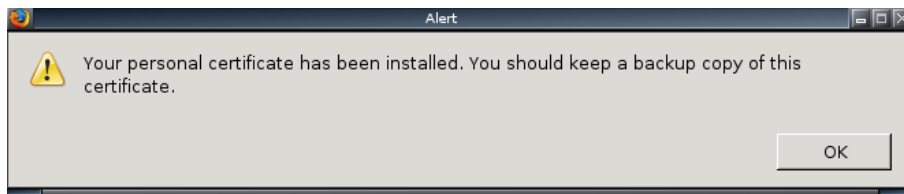
Allez sur l'interface web publique d'EJBCA :

<https://localhost:8443/ejbca/>

Puis cliquez sur : Enrôlement de certificat > Pour votre navigateur

Saisissez l'identifiant et le mot de passe entrés lors de l'étape précédente.

Sélectionnez une taille de clés de 2048 bits, puis cliquez sur « OK ».



### 6.3.3 Exportation d'un certificat d'AC

Allez sur l'interface d'administration web d'EJBCA :

<https://localhost:8443/ejbca/>

Puis, allez à la rubrique : Fonctions d'AC > Fonctions basiques

Sous le titre « AdminCA1 », cliquez sur le lien « Télécharger le fichier PEM ».

### 6.3.4 Ajout d'un certificat d'AC dans Apache

Maintenant, nous allons ajouter le certificat dans la configuration d'Apache.

Pour cela ajouter le contenu du fichier du certificat de l'AC dans le fichier suivant :

```
/etc/apache2/ssl.crt/ca-bundle.crt
```

Puis, en tant que `root` relancez Apache :

```
ejbca@server:~$ /etc/init.d/apache2 restart
```

Apache est déjà configuré pour requérir un certificat client.

## 7 Compléments

### 7.1 Introduction à la cryptographie

---

Afin de se perfectionner sur les principes des infrastructures de gestion de clés, il peut être intéressant de lire une introduction à la cryptographie et notamment la cryptographie à clé publique.

### 7.2 Prochaines étapes après ce cours

---

Tout d'abord, il est recommandé de suivre la formation EJBCA Administration dans laquelle vous apprendrez à paramétrer EJBCA pour, par exemple, faire des profils de certificats, créer des AC, etc.

Après cela, vous pouvez également suivre la formation EJBCA Utilisations avancées dans laquelle vous apprendrez à faire des installations couvrant de nombreux cas réels.

## 8 Sigles et acronymes

Sigle	Désignation
AC	Autorité de certification
ACI	Access Control Instruction
AE	Autorité d'enregistrement
AEL	Autorité d'enregistrement locale
ARL	Authority Revocation List
ASCII	American Standard Code for Information Interchange
BER	Basic Encoding Rules
CA	Certificate Authority
CMP	Certificate Management Protocol
CMS	Cryptographic Message Syntax
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CQ	Certificat qualifié
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
CSR	Certificate Signing Request
CSV	Comma Separated Value
CVC	Card Verification Code
CVV	Card Verification Value
DB	Database
DC	Domain Component
DER	Distinguished Encoding Rules
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des pratiques de certification
EAR	Enterprise Archive
ECDSA	Elliptic Curve Digital Signature Algorithm
eID	Electronic Identity (Card)
EJB	Enterprise JavaBeans
EJBCA	EJB Certificate Authority
ETSI	European Telecommunications Standards Institute
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over SSL
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICP	Infrastructure à clé publique [fr-CA]
ID	Identifiant [en], Identifiant [fr]

<b>Sigle</b>	<b>Désignation</b>
IETF	Internet Engineering Task Force
IGC	Infrastructure de gestion de clés [fr-FR]
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
J2EE	Java 2 Enterprise Edition
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JDK	J2SE Development Kit
JKS	Java Key Store
JNDI	Java Naming and Directory Interface
JSF	Java Server Faces
JSP	Java Server Page
LAR	Liste des autorités révoquées
LBE	LDAP Browser Explorer
LCR	Liste des certificats révoqués
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LDIF	LDAP Data Interchange Format
MD5	Message Digest 5
MGF1	Mask Generation Function 1
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PC	Politique de certification
PDC	Primary Domain Controller (Microsoft Windows NT Server)
PEM	Privacy Enhancement for Internet Electronic Mail
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure [en-US], [en]
PKIX	Public Key Infrastructure for X.509 certificates
PUK	Personal Unblocking Key
QC	Qualified Certificate
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman (algorithme asymétrique)
SCEP	Simple Certificate Enrollment Protocol
SHA-1	Secure Hash Algorithm One
SHA-256	Secure Hash Algorithm 256
SLES	Suse Linux Enterprise Server
SP	Service de publication

<b>Sigle</b>	<b>Désignation</b>
SQL	Structured Query Language
SSL	Secure Socket Layer protocol
SVG	Scalable Vector Graphics
TCP	Transmission Control Protocol
TLS	Transport Layer Security protocol
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format
XKMS	XML Key Management Specification
XML	Extensible Markup Language

## 9 Références documentaires

### Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE

### Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB
EJBCA:HOME	EJBCA - The J2EE Certificate Authority - Home	en-US	<a href="http://www.ejbca.org/">http://www.ejbca.org/</a>
EJBCA:MANUAL	EJBCA - The J2EE Certificate Authority - User Guide	en-US	<a href="http://www.ejbca.org/manual.html">http://www.ejbca.org/manual.html</a>
EJBCA:SF	SourceForge.net: J2EE Certificate Authority, EJBCA	en-US	<a href="http://sourceforge.net/projects/ejbca/">http://sourceforge.net/projects/ejbca/</a>
PRIMEKEY:DOCS	PrimeKey Solutions AB   Online Documentation	en-US	<a href="http://docs.primekey.se/documentation/en.html">http://docs.primekey.se/documentation/en.html</a>