



DIRECTION GÉNÉRALE DES IMPÔTS
DIRECTION GÉNÉRALE DE LA COMPTABILITÉ PUBLIQUE

Documentation d'installation du SVC de niveau 2.5

060818

Version 0.12

Circuit de validation

	Nom	Organisation	Date	Visa
Rédigé par :	Yannick Quenec'hdu	Architecte	21/11/06	
Vérifié par :	Jérôme Lubrez	Chef de projet		
Approuvé par :				

Historique des évolutions

Ver	Date	Auteur	Justificatif
0.10	21/11/2006	Yannick Quenec'hdu	Création du document
0.11	14/12/2006	Jérôme Lubrez	Modifications mineures suite à la relecture et l'application lors de la migration du SVC d'IRA de la version 2.0 à la version 2.5.
0.12	14/12/2006	Jérôme Lubrez	Ajout d'une référence au doc de migration pour documenter la migration du schéma de V2.0 à V2.5 après mise en place du schéma V2.0 de la base de données, dans le paragraphe «Créer le schéma de la base svc et les packages ».

Sommaire

Sommaire	2
1 Description de la livraison	5
2 Localisation physique des composants	6
3 Présentation du document et conventions	7
4 Première installation du SVC de niveau 2.5	8
4.1 Installation des machines de type répondeur SVC (machines SVC)	8
4.1.1 Noms des serveurs	8
4.1.2 Prérequis	8
4.1.3 Installation du répondeur.....	9
4.1.4 Configuration du répondeur	9
4.1.5 Démarrage du répondeur	10
4.1.6 Vérification du bon fonctionnement de l'installation	10
4.2 Installation de l'interface d'administration (machine ADM).....	11
4.2.1 Noms des serveurs	11
4.2.2 Prérequis	11
4.2.3 Installation de l'interface d'administration	12
4.2.4 Configuration de l'interface d'administration	12
4.2.5 Démarrage de l'interface d'administration.....	14
4.2.6 Vérification de bon fonctionnement.....	14
4.3 Installation de CRLProcess sur l'interface d'administration (machine ADM)	15
4.3.1 Prérequis	15
4.3.2 Installation du CRLProcess	15
4.3.3 Configuration du CRLProcess.....	15
4.3.4 Démarrage du CRLProcess	16
4.3.5 Vérification de bon fonctionnement.....	16
4.4 Installation de CRLFinder sur l'interface d'administration (machine ADM)	16
4.4.1 Prérequis	16
4.4.2 Installation du CRLFinder.....	16
4.4.3 Configuration du CRLfinder.....	17
4.4.4 Démarrage du CRLProcess	17
4.4.5 Vérification de bon fonctionnement.....	17
4.5 Installation du WebService (machine SVC).....	18
4.5.1 Prérequis	18
4.5.2 Installation du WebService.....	18
4.5.3 Configuration du WebService	18
4.5.4 Démarrage du WebService	19
4.5.5 Vérification de bon fonctionnement.....	19

4.6	Installation des bases de données	20
4.6.1	Installation Unix et réseau	20
4.6.2	Installation Oracle.....	20
4.6.3	Configuration de la base	21
4.6.4	Démarrage	26
4.6.5	Vérification de bon fonctionnement.....	27
4.6.6	Import des données.....	28
4.6.7	Compte de l'utilisateur Oracle	29
4.6.8	Arrêt de la base	29
5	Installation de plusieurs applications sur une même machine	30
6	Mise à jour d'une application.....	31
7	Procédure de retour arrière	32
8	Modification d'un certificat serveur.....	33
8.1	Conversion de fichier	33
8.2	Installation du certificat serveur sur le SVC	34

1 Description de la livraison

Ce document concerne l'installation d'un SVC 2.5 sur des machines vierges ou une mise à jour d'une version de SVC 2.5 vers une autre version de SVC 2.5. Pour une migration d'un SVC 2.0 à un SVC 2.5, il existe un document « Procédure de migration du SVC niveau 2 au niveau 2.5 ».

Packages applicatifs (répertoire RPMS)

Nom du package	Description
SVC_Responders<version>.noarch.rpm	Répondeur SVC
SVC_CRLProcess<version>.noarch.rpm	Composant CRLProcess
SVC_CRLFinder<version>.noarch.rpm	Composant CRLFinder
SVC_WebAdmin<version>.noarch.rpm	Composant Interface d'administration
SVC_WebService<version>.noarch.rpm	Composant WebService
correctif_jboss.tgz	Modification de configuration pour log4j
svc-bouncycastle-1.23-3tis.noarch.rpm	Cryptographie
svc-codec-2.04-1tis.noarch.rpm	Codec OCSP
svc-common-2.50-1tis.noarch.rpm	Librairies techniques transverses
svc-commons-fileupload-1.0-2tis.noarch.rpm	Envoi de fichier sur un serveur distant
svc-commons-lang-2.0-3tis.noarch.rpm	Outils apache
svc-dom4j-1.4-1tis.noarch.rpm	Manipulation XML
svc-mibble-2.3-4tis.noarch.rpm	API SNMP
svc-ojdbc-14-3tis.noarch.rpm	Accès Oracle JDBC
svc-taglibs-xtags-1.0.N20031211-3tis.noarch.rpm	Partie graphique de XSQL
svc-thales-xsql-utils-jboss-1.2-1tis.noarch.rpm	Utilitaires XSQL pour le SVC
svc-Xerces-2.6.2-2tis.noarch.rpm	Manipulation de XML
jakarta-commons-httpclient-2.0-0.rc3.1jpp.noarch.rpm	Composant Jakarta : client HTTP

Fichiers de configuration (répertoire conf)

server.xml	Fichier de configuration pour Tomcat
correctif_jboss_service.tgz	Modification jboss-service.xml
correctif_jboss.tgz	Modification des niveaux de log log4j de JBoss
mod_jk.conf	Configuration de mod_jk
workers1.properties	Configuration de mod_jk
httpd.conf	Configuration d'Apache
jboss.conf	Configuration de Jboss

2 Localisation physique des composants

Les composants SVC doivent être installés selon les règles suivantes :

- SVC_Responders et SVC_WebService s'installent chacun sur chaque machine d'ensemble en front-office derrière les Altéon (machine SVC),
- SVC_CRLFinder, SVC_CRLProcess et SVC_WebAdmin s'installent sur la même machine physique (machine ADM), différente des machines SVC_Responders, disposant d'une sortie vers Internet

Il est nécessaire d'avoir installé et démarré la base de données avant de démarrer l'ensemble de ces applications.

3 Présentation du document et conventions

Pour chacun des types de machine, le document décrit :

- les prérequis avant installation,
- l'installation initiale,
- les commandes de démarrage,
- la vérification de bonne installation.

La réinstallation d'une nouvelle version d'un package préalablement installée est décrite au chapitre 6 - Mise à jour d'une application.

Les lignes de commande respectent le formalisme suivant :

: prompt pour toute commande à effectuer sous l'utilisateur root. exemple :

```
# service httpd stop
```

> : prompt pour toute commande à effectuer sous un utilisateur spécifique (autre que root). exemple :

```
> ls -l
```

Le document ne décrit pas les méthodes pour modifier les mots de passe par défaut des utilisateurs :

- root sous Unix
- sys, system et svc sous Oracle

4 Première installation du SVC de niveau 2.5

Ce document concerne l'installation d'un SVC 2.5 sur des machines vierges ou une mise à jour d'une version de SVC 2.5 vers une autre version de SVC 2.5. Pour une migration d'un SVC 2.0 à un SVC 2.5, il existe un document « Procédure de migration du SVC niveau 2 au niveau 2.5 ».

4.1 Installation des machines de type répondeur SVC (machines SVC)

4.1.1 Noms des serveurs

Au CSI de Lyon les 3 serveurs concernés sont :

SVC2SRV-01, SVC2SRV-02 et SVC2SRV-03.

Au CSI de Bordeaux les 7 serveurs concernés sont :

SVCSRV-01, SVCSRV-02, SVCSRV-03, SVCSRV-04, SVCSRV-05, SVCSRV-06 et SVCSRV-07.

[YQU1]Ces serveurs sont appelés SVC dans la documentation.

4.1.2 Prérequis

- Disposer du master J2EE 2004 (socle version ≥ 1.41 en cas de serveur Bull, version ≥ 1.42 en cas de serveur IBM) profil sj2eeweb et des packages RPM du SVC version 2
- Connaître l'adresse IP de la machine qui doit recevoir les traps SNMP
- Connaître l'adresse IP de la base de données (machine Oracle)

Installer le master J2EE 2004 sur la machine cible

Se connecter en tant que root sur la machine concernée.

Définir le dossier contenant les sources d'installation du SVC :

- Cas d'un répertoire local (exemple : /tmp)

```
# export SVCINSTALL=/tmp/svc2.5
```

- Cas d'un CD-ROM

```
# export SVCINSTALL=/mnt/cdrom/svc2.5/
```

Arrêter les services JBoss et Apache

```
# service httpd stop  
# service jboss stop
```

Configurer mod_jk

Apache étant utilisé comme serveur Web, le connecteur mod_jk est utilisé pour la communication entre Apache et Tomcat. Il est nécessaire de le configurer :

- Fichier /etc/httpd/conf/workers1.properties :

Ce fichier est livré dans le répertoire des fichiers de configuration (svc2.0/conf/workers1.properties).

```
# cp $SVCINSTALL/conf/workers1.properties  
/etc/httpd/conf/workers1.properties
```

- Fichier /etc/httpd/conf.d/mod_jk.conf :

Ce fichier est livré dans le répertoire des fichiers de configuration (svc2.0/conf/mod_jk.conf).

```
# cp $SVCINSTALL/conf/mod_jk.conf /etc/httpd/conf.d/mod_jk.conf
```

Copier la configuration Apache livrée :

```
# cp $SVCINSTALL/conf/httpd.conf /etc/httpd/conf/httpd.conf
```

Copier la configuration de Jboss du master :

```
# cp $SVCINSTALL/conf/jboss.conf /etc/jboss.conf
```

Copier le fichier de paramétrage de Tomcat

```
# cp $SVCINSTALL/conf/server.xml  
/var/jboss/server/default/deploy/jbossweb-tomcat50.sar/
```

Corriger la configuration de log4J du master :

```
# cd /var/jboss/server/default/conf/  
# tar -xvzf $SVCINSTALL/conf/correctif_jboss.tgz
```

4.1.3 Installation du répondeur

Accéder au répertoire contenant les sources à installer :

```
# cd $SVCINSTALL/RPMS
```

Installer les sources du répondeur SVC :

```
# rpm -iv jakarta-commons-httpclient-2.0-0.rc3.1jpp.noarch.rpm  
# rpm -iv svc*  
# rpm -iv SVC_Responders<version>.noarch.rpm
```

Notes :

Dans la première instruction, les lettres svc sont en minuscules.

Le terme <version> est à remplacer par la version livrée.

4.1.4 Configuration du répondeur

Editer le fichier de configuration svc.properties pour configurer SNMP :

```
# vi /var/jboss/server/default/conf/svc.properties
```

Remplacer la chaîne `snmp.host=SNMP-HOST` par `snmp.host=<adresse IP du serveur SNMP>`

Exemple : `snmp.host=192.168.100.10`

Si le port utilisé sur le serveur `snmp` n'est pas 162 modifier `snmp.port=162` en conséquence.

Editer la configuration Oracle :

```
# vi /var/jboss/server/default/deploy/oracle-ds.xml
```

Remplacer la chaîne ORACLE-HOST par l'adresse IP du serveur ORACLE :

```
[...]  
<connection-url>jdbc:oracle:thin:@ORACLE-HOST:1521:SVC</connection-url>  
[...]
```

Exemple :

```
[...]  
<connection-url>jdbc:oracle:thin:@192.168.100.11:1521:SVC</connection-url>  
[...]
```

4.1.5 Démarrage du répondeur

Démarrer Apache par la commande :

```
# service httpd start
```

Avoir démarré la base de données

Démarrer JBoss par la commande :

```
# service jboss start
```

4.1.6 Vérification du bon fonctionnement de l'installation

Observer les logs du serveur JBoss :

```
# cat /var/log/jboss/default/server.log
```

Aucun message d'erreur ne doit apparaître.

Observer les traps SNMP émises au démarrage de l'application :

```
# cat /var/log/jboss/default/snmptraps.log
```

Ceci donne un affichage du type :

```
2004-06-18 17:37:21,308 INFO [SNMP] envoi du trap :  
BDfrontoffice.BDfrontofficeOK () vers 127.0.0.1:162  
2004-06-18 17:37:21,333 INFO [SNMP] envoi du trap : PILOTE.PILOTEOK ()  
vers 127.0.0.1:162  
2004-06-18 17:37:21,351 INFO [SNMP] envoi du trap : VALREV.VALREVOK ()  
vers 127.0.0.1:162  
2004-06-18 17:37:21,354 INFO [SNMP] envoi du trap : VERCAC.VERCACOK ()  
vers 127.0.0.1:162  
2004-06-18 17:37:21,358 INFO [SNMP] envoi du trap : VERCER.VERCEROK ()  
vers 127.0.0.1:162  
2004-06-18 17:37:21,360 INFO [SNMP] envoi du trap : SIGREP.SIGREPOK ()  
vers 127.0.0.1:162
```

Effectuer un appel avec un client de test.

4.2 Installation de l'interface d'administration (machine ADM)

4.2.1 Noms des serveurs

Au CSI de Lyon les 2 serveurs concernés sont :

SVC2ADM-01 et SVC2ADM-02.

Au CSI de Bordeaux les 2 serveurs concernés sont :

SVCADM-01 et SVCADM-02.

[YQU2]Ces serveurs sont appelés ADM dans la documentation.

4.2.2 Prérequis

- Disposer du master J2EE 2004 (socle version ≥ 1.41 en cas de serveur Bull, version ≥ 1.42 en cas de serveur IBM) profil sj2eeweb et des packages RPM du SVC version 2
- Connaître l'adresse IP de la machine qui doit recevoir les traps SNMP
- Connaître l'adresse IP de la base de données (machine Oracle)

Installer le master J2EE 2004 sur la machine cible

Se connecter en tant que root sur la machine concernée.

Définir le dossier contenant les sources d'installation du SVC :

- Cas d'un répertoire local (exemple : /tmp)

```
# export SVCINSTALL=/tmp/svc2.5
```

- Cas d'un CD-ROM

```
# export SVCINSTALL=/mnt/cdrom/svc2.5/
```

Arrêter les services JBoss et Apache

```
# service httpd stop  
# service jboss stop
```

Configurer mod_jk

Apache étant utilisé comme serveur Web, le connecteur mod_jk est utilisé pour la communication entre Apache et Tomcat. Il est nécessaire de le configurer :

- Fichier /etc/httpd/conf/workers1.properties :

Ce fichier est livré dans le répertoire des fichiers de configuration (svc2.0/conf/workers1.properties).

```
# cp $SVCINSTALL/conf/workers1.properties  
/etc/httpd/conf/workers1.properties
```

- Fichier /etc/httpd/conf.d/mod_jk.conf :

Ce fichier est livré dans le répertoire des fichiers de configuration (svc2.0/conf/mod_jk.conf).

```
# cp $SVCINSTALL/conf/mod_jk.conf /etc/httpd/conf.d/mod_jk.conf
```

Copier la configuration Apache livrée :

```
# cp $SVCINSTALL/conf/httpd.conf /etc/httpd/conf/httpd.conf
```

Copier la configuration de Jboss du master :

```
# cp $SVCINSTALL/conf/jboss.conf /etc/jboss.conf
```

Copier le fichier de paramétrage de Tomcat

```
# cp $SVCINSTALL/conf/server.xml  
/var/jboss/server/default/deploy/jbossweb-tomcat50.sar/
```

Corriger la configuration de log4J du master :

```
# cd /var/jboss/server/default/conf/  
# tar -xvzf $SVCINSTALL/conf/correctif_jboss.tgz
```

Changer l'ordre de déploiement Jboss : jboss-service.xml

```
# cd /var/jboss/server/default/conf/  
# tar -xvzf $SVCINSTALL/conf/correctif_jboss_service.tgz
```

4.2.3 Installation de l'interface d'administration**Accéder au répertoire contenant les sources à installer :**

```
# cd $SVCINSTALL/RPMS
```

Installer les sources de l'interface d'administration :

```
# rpm -iv jakarta-commons-httpclient-2.0-0.rc3.1jpp.noarch.rpm  
# rpm -iv svc*  
# rpm -iv SVC_WebAdmin<version>.noarch.rpm
```

Notes :

Dans la première instruction, les lettres svc sont en minuscules.

Le terme <version> est à remplacer par la version livrée.

4.2.4 Configuration de l'interface d'administration**Editer le fichier de configuration svc.properties pour configurer SNMP :**

```
# vi /var/jboss/server/default/conf/svc.properties
```

Remplacer la chaîne `snmp.host=SNMP-HOST` par `snmp.host=<adresse IP du serveur SNMP>`

Exemple : `snmp.host=192.168.100.10`

Si le port utilisé sur le serveur `snmp` n'est pas 162 modifier `snmp.port=162` en conséquence.

Modifier l'URL du répondeur servant aux vérifications de certificats insérés :

Remplacer la chaîne `clientsvc.url=RESPONDER-HOST` par `clientsvc.url=<URL du répondeur>`

Exemple : `clientsvc.url=http://192.168.100.10/dgi/srvsvc`

Modifier l'URL du CRLFinder :

Remplacer la chaîne `java.naming.provider.url=FINDER-HOST` par
`java.naming.provider.url=<URL du CRLfinder>`

Exemple : `java.naming.provider.url=localhost`

Configurer le proxy :

Si aucun proxy n'est utilisé, il est inutile de modifier la configuration livrée. Sinon, éditer le fichier de configuration du SVC :

vi /var/jboss/server/default/conf/svc.properties

Le configurer en positionnant les champs de la section suivante de ce fichier :

#-----proxy http -----

download.proxy=true

proxy.host=PROXY-HOST

proxy.port=8080

`#proxy.username=`

`#proxy.password=`

#pas de proxy pour les noms/ip qui commencent par:

#exemple: proxy.exclude=192.168.0.,99.4.29.223,.appli.dgi

proxy.exclude=192.168.100.,.appli.dgi,.appli.impots

La ligne `proxy.exclude` ne doit en aucun cas être commentée. S'il est nécessaire de la laisser vide, la syntaxe est alors :

`proxy.exclude=`

Modifier la configuration XSQL :

vi /var/jboss/server/default/lib/xsqldir/XSQLConfig.xml

Remplacer la chaîne `ORACLE-HOST` par l'adresse IP du serveur Oracle

Exemple :

`[...]`

`<dburl>jdbc:oracle:thin:@192.168.100.11:1521:SVC</dburl>`

`[...]`

Préparer un fichier `XSQLConfig.xml` avec l'adresse IP de la base de secours. Le stocker dans le répertoire de sauvegarde `/var/tmp/backup` (à créer).

Editer la configuration Oracle :

```
# vi /var/jboss/server/default/deploy/oracle-ds.xml
```

Remplacer la chaîne ORACLE-HOST par l'adresse IP du serveur ORACLE :

```
[...]  
<connection-url>jdbc:oracle:thin:@ORACLE-HOST:1521:SVC</connection-url>  
[...]
```

Exemple :

```
[...]  
<connection-url>jdbc:oracle:thin:@192.168.100.11:1521:SVC</connection-url>  
[...]
```

4.2.5 Démarrage de l'interface d'administration

Démarrer Apache par la commande :

```
# service httpd start
```

Avoir démarré la base de données

Démarrer JBoss par la commande :

```
# service jboss start
```

4.2.6 Vérification de bon fonctionnement

Observer les logs du serveur JBoss :

```
# cat /var/log/jboss/default/server.log
```

Aucun message d'erreur ne doit apparaître.

Ouvrir un navigateur web et se connecter à l'URL :

<http://SERVEUR/svcadmin/srvadmin>

Où « SERVEUR » est l'adresse IP ou le nom DNS de la machine hébergeant l'interface d'administration.

La page d'accueil de l'interface s'administration doit apparaître (mire de connexion).

4.3 Installation de CRLProcess sur l'interface d'administration (machine ADM)

4.3.1 Prérequis

Avoir installé SVC_WebAdmin sur la machine ADM comme indiqué au paragraphe précédent.

4.3.2 Installation du CRLProcess

Arrêter les services JBoss

```
# service jboss stop
```

Accéder au répertoire contenant les sources à installer :

```
# cd $SVCINSTALL/RPMS/
```

Installer les sources du CRLProcess :

```
# rpm -iv SVC_CrlProcess<version>.noarch.rpm
```

Notes :

Le terme <version> est à remplacer par la version livrée.

4.3.3 Configuration du CRLProcess

L'application CRLProcess envoie des emails aux administrateurs habilités en cas de mauvaise récupération des CRL. Afin que l'envoi d'email ait lieu, il est nécessaire de configurer l'adresse IP du serveur SMTP dans le fichier log4j.xml. Pour cela, éditer ce fichier :

```
# vi /var/jboss/server/default/conf/svc-webadmin-log4j.xml
```

Y remplacer la chaîne SMTP-HOST par l'adresse IP du serveur SMTP :

```
[...]
<!-- ===== -->
<!-- EMAIL APPENDER -->
<!-- ===== -->
<appender name="SMTP" class="org.apache.log4j.net.SMTPAppender">
  <param name="Threshold" value="FATAL" />
  <param name="BufferSize" value="1" />
  <param name="To" value="" />
  <param name="From" value="svc.admin@gouv.fr" />
  <param name="Subject" value="serveur svc" />
  <param name="SMTPHost" value="SMTP-HOST" />
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern"
      value="%d{ABSOLUTE} %C{1} - %m%n"/>
  </layout>
</appender>
[...]
```

Exemple :

```
[...]  
    <param name="SMTPHost" value="59.2.26.60" />  
[...]
```

4.3.4 Démarrage du CRLProcess

Avoir installé le CRLFinder.

Avoir démarré la base de données

Démarrer JBoss par la commande :

```
# service jboss start
```

4.3.5 Vérification de bon fonctionnement

Observer les logs du serveur JBoss :

```
# cat /var/log/jboss/default/server.log
```

Aucun message d'erreur ne doit apparaître.

Observer les traps SNMP émises au démarrage de l'application :

```
# cat /var/log/jboss/default/snmptraps.log | grep BDbckofficeOK
```

Ceci donne un affichage du type :

```
2004-06-18 20:33:00,164 INFO [SNMP] envoi du trap :  
BDbckoffice.BDbckofficeOK () vers 127.0.0.1:162
```

4.4 Installation de CRLFinder sur l'interface d'administration (machine ADM)

4.4.1 Prérequis

Avoir installé SVC_WebAdmin sur la machine ADM comme indiqué au paragraphe précédent.

4.4.2 Installation du CRLFinder

Arrêter les services JBoss

```
# service jboss stop
```

Accéder au répertoire contenant les sources à installer :

```
# cd $SVCINSTALL/RPMS/
```

Installer les sources du CRLFinder :

```
# rpm -iv svc-bouncycastle-1.23-3tis.noarch.rpm  
# rpm -iv svc-common-2.50-1tis.noarch.rpm  
# rpm -iv SVC_CrlFinder<version>.noarch.rpm  
# rpm -iv svc-mibble-2.3-4tis.noarch.rpm
```

Notes :

Le terme <version> est à remplacer par la version livrée.

4.4.3 Configuration du CRLFinder

Configurer le proxy :

Si aucun proxy n'est utilisé, il est inutile de modifier la configuration livrée. Sinon, éditer le fichier de configuration du SVC :

```
# vi /var/jboss/server/default/conf/svc.properties
```

Le configurer en positionnant les champs de la section suivante de ce fichier :

```
#-----proxy http -----  
download.proxy=true  
    proxy.host=PROXY-HOST  
    proxy.port=8080  
    #proxy.username=  
    #proxy.password=  
  
    #pas de proxy pour les noms/ip qui commencent par:  
    #exemple: proxy.exclude=192.168.0., 99.4.29.223, .appli.dgi  
    proxy.exclude=192.168.100., .appli.dgi, .appli.impots
```

La ligne `proxy.exclude` ne doit en aucun cas être commentée. S'il est nécessaire de la laisser vide, la syntaxe est alors :

```
proxy.exclude=
```

4.4.4 Démarrage du CRLFinder

Avoir démarré la base de données

Avoir installé le CRLFinder.

Démarrer JBoss par la commande :

```
# service jboss start
```

4.4.5 Vérification de bon fonctionnement

Observer les logs du serveur JBoss :

```
# cat /var/log/jboss/default/server.log
```

Aucun message d'erreur ne doit apparaître.

Observer les traps SNMP émises au démarrage de l'application :

```
# cat /var/log/jboss/default/snmptraps.log | grep BDbckofficeOK
```

Ceci donne un affichage du type :

```
2004-06-18 20:33:00,164 INFO [SNMP] envoi du trap :  
BDbckoffice.BDbckofficeOK () vers 127.0.0.1:162
```

4.5 Installation du Webservice (machine SVC)

4.5.1 Prérequis

- Disposer d'une machine SVC comportant un répondeur SVC installé selon la procédure ci-dessus.
- Connaître l'adresse IP de la base de données (machine Oracle)
- connaître l'adresse IP du serveur ADM

Se connecter en tant que root sur la machine concernée.

Arrêter le service JBoss

```
# service httpd stop  
# service jboss stop
```

Définir le dossier contenant les sources d'installation du SVC :

- Cas d'un répertoire local (exemple : /tmp)

```
# export SVCINSTALL=/tmp/svc2.0
```

- Cas d'un CD-ROM

```
# export SVCINSTALL=/mnt/cdrom/svc2.0
```

4.5.2 Installation du Webservice

Arrêter les services JBoss

```
# service jboss stop
```

Accéder au répertoire contenant les sources à installer :

```
# cd $SVCINSTALL/RPMS
```

Installer les sources du Webservice :

```
# rpm -iv SVC_WebService<version>.noarch.rpm
```

Notes :

Le terme <version> est à remplacer par la version livrée.

4.5.3 Configuration du Webservice

Editer le fichier de configuration fourni

```
# vi /var/jboss/server/default/conf/svc-webservice.properties
```

Configurer le pilote JDBC pour l'accès à la base de données

Remplacer ORACLE-HOST par l'adresse IP du serveur Oracle :

```
jdbc.url=jdbc:oracle:thin:@ORACLE-HOST:1521:SVC
```

Exemple :

```
jdbc.url=jdbc:oracle:thin:@192.168.100.11:1521:SVC
```

Définir l'adresse IP du CRLProcess

Remplacer PROCESS-HOST par l'adresse IP du serveur ADM :

```
crl.httpspath.web.archive=http://PROCESS-HOST/crl
```

Exemple :

```
crl.httpspath.web.archive=http://192.168.100.13/crl
```

Configurer le proxy :

Si aucun proxy n'est utilisé, il est inutile de modifier la configuration livrée. Sinon, le configurer en positionnant les champs de la section suivante :

```
#-----proxy http -----
download.proxy=true
    proxy.host=PROXY-HOST
    proxy.port=8080
    #proxy.username=
    #proxy.password=

    #pas de proxy pour les noms/ip qui commencent par:
    #exemple: proxy.exclude=192.168.0.,99.4.29.223,.appli.dgi
    proxy.exclude=192.168.100.,.appli.dgi
```

4.5.4 Démarrage du Webservice

Démarrer Apache par la commande :

```
# service httpd start
```

Avoir démarré la base de données

Démarrer JBoss par la commande :

```
# service jboss start
```

4.5.5 Vérification de bon fonctionnement

Observer les logs du serveur JBoss :

```
# cat /var/log/jboss/default/server.log
```

Aucun message d'erreur ne doit apparaître.

Effectuer un appel avec un client de test.

4.6 Installation des bases de données

4.6.1 Installation Unix et réseau

L'installation du SVC nécessite au moins deux serveurs de données, appelés « serveurs Oracle » dans la documentation.

Un serveur de sauvegarde peut être utilisé en complément optionnellement. Le principe sous-jacent est d'avoir si nécessaire un serveur de secours global sur la plate-forme SVC, capable de remplacer rapidement tout serveur en cas de nécessité. La procédure d'installation la plus délicate étant celle du serveur de données, on installe ce serveur de secours comme une troisième base de données. Ce serveur n'est pertinent à ce jour que sur la plate-forme CFS-Part du CSI de Bordeaux. Pour le CFS-Pro, Il n'existe pas au CSI de Lyon.

Au CSI de Lyon les 2 serveurs concernés sont :

SVC2BDD-01 et SVC2BDD-02 (serveurs Oracle).

Au CSI de Bordeaux les 3 serveurs concernés sont :

SVCDB-01, SVCDB-02 (serveurs Oracle) et SVCSAV-01 (serveur de sauvegarde).

Tous ces serveurs ont la même adresse IP sur la patte `eth0` « front-office ». Une seule des trois interfaces doit être active (`up`) à un moment donné.

La modification momentanée de l'état d'une interface s'effectue avec les commandes `ifup` et `ifdown`. La modification permanente de cet état s'effectue par modification du paramètre `ONBOOT` dans le fichier de configuration `/etc/sysconfig/network-scripts/ifcfg-eth0` pour l'interface `eth0`.

Lors de l'installation initiale, seule l'interface `eth0` du serveur Oracle 01 doit être configurée `up` de façon permanente.

4.6.2 Installation Oracle

Disposer du master J2EE 2004 (socle version ≥ 1.41 en cas de serveur Bull, version ≥ 1.42 en cas de serveur IBM) profil `soracle`

Installer Oracle avec le master Oracle.

Positionner `ORACLE_SID=svc` dans le fichier `.bashrc` de l'utilisateur Oracle.

Modifier les mots de passe par défaut de l'utilisateur `oracle` sous Unix et de l'utilisateur `sys` sous `oracle`.

Définir le dossier contenant les sources d'installation du SVC :

- Cas d'un répertoire local (exemple : `/tmp`)

```
# export SVCINSTALL=/tmp/svc2.0
```

- Cas d'un CD-ROM

```
# export SVCINSTALL=/mnt/cdrom/svc2.0
```

4.6.3 Configuration de la base

Description de la livraison

La livraison contient les répertoires et fichiers suivants :

db	backup	common.pl	configuration et fonctions transverses
		hotarch.pl	script d'archivage
		hotrest.pl	script de restauration
	base_svc	CreateDB.sql	commandes de création de la base de données
		CreateDBCatalog.sql	script de création du catalogue
		CreateDBFiles.sql	script de création des fichiers de données
		init.ora	initialisation d'Oracle
		postDBCcreation.sql	commandes post-création de l'instance SVC
		svc.sh	script de création de l'instance SVC
	oracle	listener.ora	configuration du Listener
		oracle	script de démarrage Oracle et listener
		oratab	démarrage automatique de l'instance SVC
		tnsnames.ora	configuration des noms sur la base active
	schema	create_usersvc.sql	commandes de création du user SVC
		crinfo.sql	procédures stockées liées aux CRL
		schema_svc.sql	schéma de l'instance SVC
		validation.sql	procédures stockées liées à la validation de données

Note : la mise en oeuvre des scripts d'archivage et de restauration est détaillée dans la documentation d'exploitation.

Préparer les répertoires et la configuration

Se connecter en tant que root sur le serveur

L'installation est effectuée directement sous /var/base pour éviter de saturer le filesystem / .

Créer les répertoires /base/admin/svc/scripts , /base/admin/svc/schema et /base/admin/svc/oracle, et leur affecter les droits nécessaires :

```
# mkdir /var/base
# ln -s /var/base /base
# ls -l /var/base
Vérifier que les droits sont (root, root, 755), sinon corriger
# cd /base
# mkdir admin
# cd admin
# mkdir svc
# cd svc
# mkdir scripts
# mkdir schema
# mkdir oracle
# chown -R oracle:dba /base/admin
```

Créer le répertoire /base/oradata

```
# cd /base
# mkdir oradata
# chown -R oracle:dba /base/oradata
```

Se connecter en tant qu'utilisateur oracle sur le serveur.

```
# su - oracle
```

Identifier le répertoire contenant les données à installer

```
> export SVCINSTALL=/tmp/svc2.0 (cas d'un répertoire local)
> export SVCINSTALL=/mnt/cdrom/svc2.0 (cas d'un CD-ROM)
```

Copier les fichiers en local sur /tmp

```
> cp -a $SVCINSTALL/db/ /tmp
```

Vérifier que les fichiers copiés appartiennent à l'utilisateur unix oracle/dba, sinon, en tant que root, exécuter la commande suivante :

```
# chown -R oracle:dba /tmp/db
# chmod -R 755 /tmp/db
```

En tant qu'oracle, copier les fichiers du répertoire /tmp/db/base_svc/ dans le répertoire /base/admin/svc/scripts/

```
> cp /tmp/db/base_svc/* /base/admin/svc/scripts/  
> ls -l /base/admin/svc/scripts/
```

Vérifier que les droits sont (oracle, dba, 755), sinon corriger.

En tant qu'oracle, copier les fichiers du répertoire /tmp/db/schema/ dans le répertoire /base/admin/svc/schema/

```
> cp /tmp/db/schema/* /base/admin/svc/schema/  
> ls -l /base/admin/svc/schema/
```

Vérifier que les droits sont (oracle, dba, 755), sinon corriger.

En tant qu'oracle, copier les fichiers du répertoire /tmp/db/oracle/ dans le répertoire /base/admin/svc/oracle/

```
> cp /tmp/db/oracle/* /base/admin/svc/oracle/  
> ls -l /base/admin/svc/oracle/
```

Vérifier que les droits sont (oracle, dba, 755), sinon corriger.

Créer la base SVC

Modifier si nécessaire les mots de passe Oracle de sys et system après installation et vérifier les répertoires utilisés dans les scripts. Les scripts livrés utilisent les mots de passe par défaut de l'installation d'Oracle.

Le contenu du script svc.sh est le suivant :

```
#!/bin/sh  
mkdir /base/admin/svc/bdump  
mkdir /base/admin/svc/cdump  
mkdir /base/admin/svc/create  
mkdir /base/admin/svc/pfile  
mkdir /base/admin/svc/udump  
mkdir /base/oradata/svc  
mkdir /oracle/ora920/dbs  
export ORACLE_SID=svc  
echo Ajouter cette entrée dans oratab : svc :/oracle/ora920 :Y  
/oracle/ora920/bin/orapwd file=/oracle/ora920/dbs/orapwsvc  
password=change_on_install  
/oracle/ora920/bin/sqlplus /nolog @/base/admin/svc/scripts/CreateDB.sql  
/oracle/ora920/bin/sqlplus /nolog  
@/base/admin/svc/scripts/CreateDBFiles.sql  
/oracle/ora920/bin/sqlplus /nolog  
@/base/admin/svc/scripts/CreateDBCatalog.sql  
/oracle/ora920/bin/sqlplus /nolog  
@/base/admin/svc/scripts/postDBCcreation.sql
```

Dans ce fichier, le mot de passe `change_on_install` est le mot de passe par défaut du compte

sys, qui est créé à l'installation d'Oracle. Si ce mot de passe n'est pas modifié lors de l'installation du master, on ne doit pas le changer non plus dans le fichier `svc.sh`.

Exécuter le script `svc.sh`, ce qui exécute la création de la base `svc`

```
> cd /base/admin/svc/scripts/  
> ./svc.sh
```

L'exécution de ce script dure environ 15 minutes et affiche des commandes Oracle et un ensemble de données numériques à l'écran. Ce comportement est normal.

A la fin de l'exécution, le prompt SQL apparaît et il suffit de taper la commande `exit` pour revenir au shell :

```
SQL> exit  
>
```

Si le script s'arrête en cours d'exécution et demande la valeur pour `owa_file_var`, saisir `/oracle/ora920/rdbms/admin/owadummy.sql` (ceci est un bug de oracle)

On peut vérifier la bonne exécution du script en consultant les fichiers de log dans le répertoire `/oracle/ora920/assistants/dbca/logs/`

Vérifier que les fichiers de base de données sont créés dans le répertoire `/base/oradata/svc/`

Copier le fichier `init.ora` dans le répertoire `/oracle/ora920/dbs/initsvc.ora` :

```
> cp /base/admin/svc/scripts/init.ora /oracle/ora920/dbs/initsvc.ora  
> ls -l /oracle/ora920/dbs/initsvc.ora
```

Vérifier que les droits sont (oracle, dba, 755), sinon corriger.

Modifier le fichier `/etc/oratab` pour faire en sorte que la base démarre automatiquement, en exécutant la commande :

```
> vi /etc/oratab
```

Commenter les lignes éventuellement présentes et ajouter la ligne suivante, si elle n'est pas présente :

```
svc:/oracle/ora920:Y
```

Vérifier les droits sur ce fichier, ils doivent être (oracle, dba, 664), sinon corriger.

Copier le fichier `listener.ora` dans le répertoire `/oracle/ora920/network/admin`

```
> cp /tmp/db/oracle/listener.ora /oracle/ora920/network/admin/listener.ora  
> ls -l /oracle/ora920/network/admin/listener.ora
```

Vérifier que les droits sont (oracle, dba, 755), sinon corriger.

Vérifier que les adresses IP des interfaces sont les mêmes que celles déclarées dans le `/etc/hosts` précédemment, sinon le mettre à jour. Pour cela :

Remplacer « `itf_svc` » par l'adresse IP du serveur BDD sur le réseau MiddleEnd

Remplacer « `itf_adm` » par l'adresse IP du serveur BDD sur le réseau BackEnd

Dans « `SID_LIST_LISTENER` » ajouter :

```
(SID_DESC =  
  (GLOBAL_DBNAME = svc)  
  (ORACLE_HOME = /oracle/ora920)  
  (SID_NAME = svc)  
)
```

Note : sur la base de secours, on laisse la configuration sur l'interface SVC même si celle-ci est tombée. Ceci ne pose aucun problème car la base de secours n'est pas démarrée, et ceci permet de simplifier la procédure de bascule.

Copier le fichier tnsnames.ora dans le répertoire /oracle/ora920/network/admin

```
> cp /tmp/db/oracle/tnsnames.ora /oracle/ora920/network/admin/  
> ls -l /oracle/ora920/network/admin/tnsnames.ora
```

Vérifier que les droits sont (oracle, dba, 755), sinon corriger.

Vérifier que les adresses IP des interfaces sont les mêmes que celles déclarées dans le /etc/hosts précédemment, sinon le mettre à jour. Pour cela :

```
Remplacer « itf_svc » par l'adresse IP du serveur BDD sur le réseau  
MiddleEnd  
Remplacer « itf_adm » par l'adresse IP du serveur BDD sur le réseau BackEnd  
Remplacer :  
(CONNECT_DATA =  
  (SERVICE_NAME = svc)  
par :  
(CONNECT_DATA =  
  (SID = svc)  
  (SERVICE_NAME = svc)
```

Note : sur la base de secours, on laisse la configuration sur l'interface SVC même si celle-ci est tombée. Ceci ne pose aucun problème car la base de secours n'est pas démarrée, et ceci permet de simplifier la procédure de bascule.

En tant que root, copier le fichier « oracle » dans le répertoire /etc/init.d :

```
# cp /tmp/db/oracle/oracle /etc/init.d/  
# ls -l /etc/init.d/oracle
```

Vérifier que les droits sont (root, root, 755), sinon corriger.

Dans ce fichier « oracle », remplacer le cas échéant « dbshut immediate » par « dbshut ».

Dans le fichier /oracle/ora920/bin/dbshut, ajouter « immediate » après la commande « shutdown » pour la version d'Oracle en cours.

Sur la base active, mettre la base Oracle en démarrage automatique au boot de la machine :

```
# cd /etc/init.d/  
# chkconfig --add oracle
```

```
# chkconfig --list | grep oracle
oracle    0:Arrêt  1:Arrêt  2:Arrêt  3:Marche  4:Marche  5:Marche  6:Arrêt
```

Sur la base de secours, Oracle doit être arrêté de façon permanente.

Paramétrage de la base de données

Pour le CSI de Bordeaux uniquement, positionner les statistiques (on peut utiliser les mêmes outils que ceux développés pour ADONIS V2, en les paramétrant pour la base svc). Automatiser leur calcul toutes les nuits (ceci peut être chaîné à l'exécution du script hotarch.pl).

Créer le répertoire /home/oracle/outils_DBA et y placer les outils transverses d'administration Oracle disponibles au CSI.

Inclure ce répertoire dans les sauvegardes SVC (cf. dossier d'exploitation).

Mettre en place la rotation des logs sur les fichiers listener.log et alert.log

Mettre en place la purge des fichiers *.trc (fichiers de trace) et archivelog, dans le crontab oracle :

- au CSI de Bordeaux, reprendre les procédures ADONIS)
- au CSI de Lyon, reprendre les procédures transverses développées par le CSI pour SVC V1.

4.6.4 Démarrage

Redémarrer la base de données :

Se connecter en tant que `root` et exécuter la commande :

```
# service oracle restart
```

Créer l'utilisateur svc sur la base svc

Se connecter en tant qu'utilisateur oracle, et aller dans le répertoire /tmp/db/schema

```
# su - oracle
> cd /tmp/db/schema
```

Se connecter sur la base en tant que `system` et exécuter le script « `create_usersvc.sql` »

```
> sqlplus system/manager@svc
SQL>@create_usersvc.sql
SQL>exit
>
```

Créer le schéma de la base svc et les packages

Se connecter sur la base en tant que `svc` et exécuter les scripts « `schema_svc.sql` », « `validation.sql` » et « `crlinfo.sql` »

```
> sqlplus svc/psvc@svc
SQL>@schema_svc.sql
SQL>@validation.sql
```

```
SQL>@crlinfo.sql  
SQL>exit
```

Ces commandes créent le schéma en version 2.0. Il faut les compléter par celles de migration documenter dans le document « Procédure de migration du SVC de niveau 2 au niveau 2.5 », chapitre 2 « Migration de la base pour le SVC niveau 2.5 ».

Sur la base active (01 à la première installation), laisser Oracle démarré.

Sur la base de secours (02 à la première installation), arrêter Oracle.

Sur le serveur de sauvegarde s'il existe, arrêter Oracle.

4.6.5 Vérification de bon fonctionnement

Afin de vérifier la bonne configuration d'Oracle, il est possible d'effectuer le test suivant lorsqu'Oracle est démarré.

Se loguer comme utilisateur Oracle sur la machine :

```
# su - oracle
```

Se connecter à SQLPLUS avec l'utilisateur Oracle svc :

```
> sqlplus svc/psvc@svc
```

On obtient l'affichage suivant :

```
SQL*Plus: Release 9.2.0.6.0 - Production on Mon Jun 21 09:27:37 2004  
  
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.  
  
Connected to:  
Oracle9i Enterprise Edition Release 9.2.0.6.0 - Production  
With the Partitioning, OLAP and Oracle Data Mining options  
JServer Release 9.2.0.6.0 - Production  
  
SQL>
```

L'affichage de la liste des tables par la commande :

```
SQL> select table_name from user_tables;
```

donne :

```
TABLE_NAME  
-----  
ADMUSR  
CA  
CATRUSTDOM  
CRL  
EXTKEYUSAGE
```

```

HASHCA
HCRL
ICRL
LOG
POLICY
POLPARAM

TABLE_NAME
-----
REFPARAM
REQUESTCRL
REVLIN
TRUSTDOM
VALDOM
VALIDATIONPOLICY
VALIDPATH
VPTRUSTDOM
SVCPARAM

20 rows selected.

```

L'affichage du contenu de la table trustdom par la commande :

```
SQL> select * from trustdom;
```

donne :

```

IDTRUSTDOM
-----
-----
NAME
-----
-----
1.2.250.1.131.1.5.4.7.1.0
SVC

```

4.6.6 Import des données

Si un export de base de données à été fourni par la MOE SVC, l'importer selon la procédure fournie. Dans le cas contraire, se référer au guide d'utilisation de l'interface d'administration afin de déclarer les AC et l'ensemble des paramètres dans la base de données du SVC.

Attention le schéma de la base de données de la version 2.0 et de la version 2.5 du SVC sont distinctes. L'importation de données d'une base SVC 2.0 dans une SVC 2.5 n'a pas été testé, ni l'inverse.

4.6.7 Compte de l'utilisateur Oracle

Pour simplifier l'exploitation, modifier le compte Oracle :

- définir la variable ORACLE_SID dans le fichier .bash_profile de l'utilisateur Oracle. Elle prend la valeur svc.
- modifier le répertoire home de connexion d'Oracle en /home/oracle après avoir créé ce répertoire.

4.6.8 Arrêt de la base

Pour arrêter la base, se connecter en tant que `root` et exécuter la commande

```
# service oracle stop
```

Ceci arrête la base et le listener.

5 Installation de plusieurs applications sur une même machine

Il est possible d'installer plusieurs applications sur la même machine, par exemple de faire cohabiter un répondeur avec l'application CRLProcess. Ceci n'est pas recommandé en production pour des raisons de performances, mais est tout à fait acceptable pour des tests fonctionnels.

Dans ce cas, il suffit de suivre les procédures d'installation décrites dans le présent document, avec les deux consignes complémentaires suivantes :

Installation du second package

Lors de l'exécution de la seconde commande `rpm -iv`, la commande refuse de s'exécuter en raison d'un conflit de fichiers de configuration. On peut forcer l'installation en ajoutant à la commande `rpm` l'option `--force` :

```
# rpm -iv --force <nom du package.rpm>
```

Fusion des fichiers de configuration

Cette installation crée, pour chacun des fichiers de configuration en conflit, un fichier de configuration d'extension `.rpmnew` dans le même répertoire que le fichier en conflit.

Pour chacun de ces fichiers, il est nécessaire de les fusionner en un seul dans lequel chaque information de configuration est présente une fois et une seule et correctement renseignée, et de supprimer du disque le fichier `.rpmnew` créé.

Les fichiers susceptibles d'être en conflit sont :

- `svc.properties.xml`
- `oracle-ds.xml`
- `svc-<package>-log4j.xml`

6 Mise à jour d'une application

Ce document concerne l'installation d'un SVC 2.5 sur des machines vierges ou une mise à jour d'une version de SVC 2.5 vers une autre version de SVC 2.5. Pour une migration d'un SVC 2.0 à un SVC 2.5, il existe un document « Procédure de migration du SVC niveau 2 au niveau 2.5 ».

Lors de la livraison d'une nouvelle version d'une application, la mise à jour d'une application préalablement installée s'effectue par les commandes suivantes, à effectuer sur chaque serveur d'application (et non sur les serveurs de données).

L'arrêt de JBoss est obligatoire, il évite les difficultés que peut éprouver JBoss avec le remplacement à chaud des EAR.

```
# service jboss stop
```

Si l'on souhaite vérifier quels composants SVC sont déjà présents sur la machine, on peut utiliser la commande suivante :

```
# rpm -qa | grep -i SVC
```

La mise à jour s'effectue par la procédure suivante :

- copier localement l'ensemble des RPMs livrés,
- se placer dans le répertoire les contenant,
- depuis ce répertoire, appliquer la commande :

```
# rpm -Fvh svc* SVC*
```

Cette commande garantit que seuls les packages déjà présents sur le serveur sont mis à jour.

Il ne faut ensuite effectuer aucune des actions de configuration décrites dans la procédure d'installation, sauf si le bordereau d'accompagnement le précise.

Si les fichiers de configuration ont évolué depuis l'installation précédente, la commande `rpm` le signale sur sa sortie standard, et les nouveaux fichiers de configuration sont placés dans des fichiers de même nom, d'extension `.rpmnew`, situés dans le même répertoire.

Si le bordereau ne spécifie pas de modifier ces fichiers par rapport à la version précédente, il suffit de les supprimer.

Il est alors possible de redémarrer JBoss par la commande :

```
# service jboss start
```

et d'appliquer les vérifications de bon fonctionnement décrits dans le chapitre d'installation initiale correspondant au composant mis à jour.

7 Procédure de retour arrière

Lors de la livraison d'une nouvelle version d'une application, la mise à jour décrite au paragraphe précédent peut dysfonctionner.

Dans ce cas, il est nécessaire de réinstaller la version applicative préalablement en production.

L'arrêt de JBoss est obligatoire, il évite les difficultés que peut éprouver JBoss avec le remplacement à chaud des EAR.

```
# service jboss stop
```

Si l'on souhaite vérifier quels composants SVC sont déjà présents sur la machine, on peut utiliser la commande suivante :

```
# rpm -qa | grep -i SVC
```

Le retour arrière s'effectue par la procédure suivante :

- appliquer la commande de désinstallation :

```
# rpm -e svc* SVC*
```

- appliquer la procédure d'installation complète de la version logicielle à laquelle on veut revenir, en se référant au chapitre 4 « Première installation du SVC de niveau 2 » du présent document.

8 Modification d'un certificat serveur

Lors du processus d'installation des répondeurs SVC et de l'interface d'administration, un certificat serveur et sa clé privée sont déployés pour réaliser la signature des réponses.

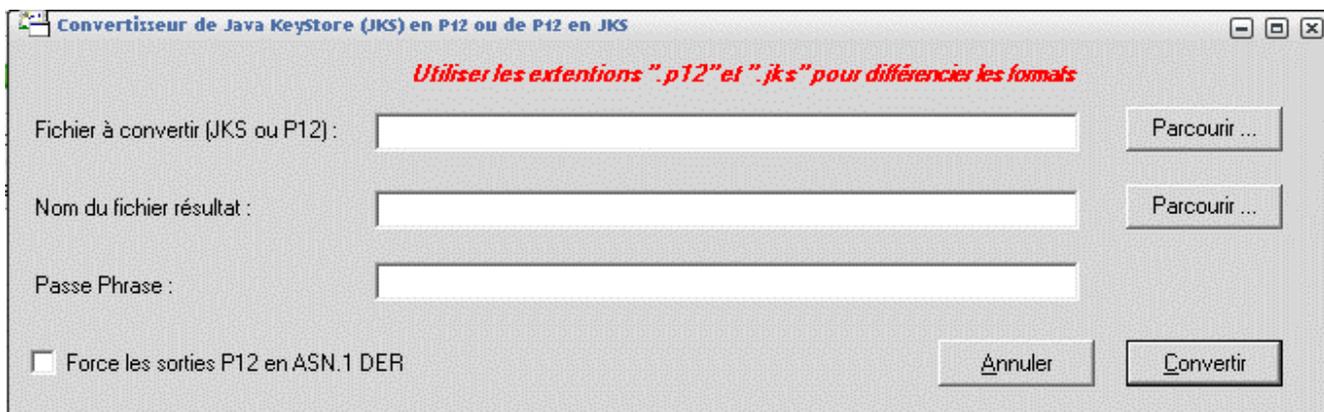
En cas de fin de vie ou de compromission du certificat serveur, il devra être remplacé par un nouveau certificat valide. La procédure suivante décrit le processus pour modifier le certificat serveur du SVC.

Le format de protection du certificat et de la clé privée peut être soit au format PKCS12 ou au format JKS. Dans le cas où celui-ci serait au format PKCS12, il est nécessaire de commencer la procédure à partir de l'étape 7.1, si le fichier est au format JKS vous devez commencer la procédure à partir de l'étape 7.2

8.1 Conversion de fichier

Le format de protection du certificat et de sa clé doit être au format JKS (Java KeyStore). C'est actuellement le seul format accepté par le SVC. En revanche, le mode de diffusion le plus courant est le format PKCS12. Si vous utilisez des fichiers PKCS12, il est nécessaire de transformer ce fichier au format JKS. Pour ce faire, le SVC fournit dans le répertoire *utils*, un utilitaire permettant depuis un poste Windows de transformer le fichier P12 vers JKS ou inversement. Préalablement, il est nécessaire d'installer la librairie Docnet fournie dans le répertoire *utils* pour exécuter ce programme.

L'utilitaire se nomme JKSP12. Pour réaliser la transformation, il est nécessaire d'exécuter le programme JKSP12, l'interface suivante apparaît :



- Importer le fichier PKCS12 à convertir
- Indiquer le nom du fichier et le répertoire de sortie du fichier JKS
- Saisir le mot de passe du fichier PKCS12.
- Appuyer sur le bouton convertir

8.2 Installation du certificat serveur sur le SVC

Dans le cas de la livraison d'une version applicative complète du SVC, le certificat serveur et le modèle de fichier de configuration `svc-crypto.properties` sont fournis à la racine de la livraison, dans le répertoire `crypto`.

Dans les autres cas, ils peuvent faire l'objet d'une livraison séparée.

Les serveurs concernés sont : tous les répondeurs SVCSRVR et la console d'administration ADM.

La procédure suivante décrit le processus d'installation du certificat serveur et de sa clé privée si ceux-ci sont encapsulés dans un format JKS.

Elle s'applique sur tous les serveurs concernés.

Elle prend comme exemple le cas où le fichier JKS est nommé `svcv2.jks`.

- Arrêter JBOSS :

```
# service jboss stop
```

- Définir le répertoire contenant le certificat serveur :

Cas d'un répertoire local (exemple /tmp) :

```
# export CERTINSTALL=/tmp/clientTest/certs/
```

Cas d'un CD-ROM ou de l'ISO SVC2.11.iso

```
# export CERTINSTALL=/mnt/cdrom/crypto/
```

- Placer le fichier keystore (JKS) sur les répondeurs SVC et l'interface d'administration, dans le répertoire `/var/jboss/server/default/conf`

```
# cp $CERTINSTALL/svcv2.jks /var/jboss/server/default/conf/
```

- Sauvegarder le fichier de configuration dans `/var/tmp`:

```
cp /var/jboss/server/default/conf/svc-crypto.properties /var/tmp/svc-crypto.properties_date_du_jour
```

- Dans le répertoire `/var/jboss/server/default/conf`, éditer le fichier `svc-crypto.properties` :

- KEYSTORE doit pointer sur le nom du fichier (dans notre exemple : `svcv2.jks`)

```
KEYSTORE=${jboss.server.home.dir}/conf/svcv2.jks
```

- PASSPHRASE doit valoir le mot de passe choisi

```
PASSPHRASE=<motdepasse>
```

- ALIAS doit valoir le nom donné à l'alias de certificat (exemple : `svcalias`). Si l'alias vous est inconnu, il est possible d'utiliser la ligne de commande suivante depuis le répondeur SVC ou depuis l'interface d'administration pour le connaître :

- keytool -list -v -keystore svcv2.jks.
- Saisir le mot de passe du JKS
- L'alias est celui indiqué juste au dessus de la ligne certificat[1]

```
ALIAS=svcv2
```

- DESTROY doit valoir true ou false. S'il est true, le mot de passe PASSPHRASE est supprimé du fichier au démarrage de JBoss et doit être resaisi manuellement dans le fichier à chaque redémarrage. Ceci garantit la confidentialité du mot de passe et empêche le redémarrage du serveur par une personne non autorisée. S'il est false, le mot de passe PASSPHRASE n'est pas supprimé du fichier au démarrage de JBoss.

```
DESTROY=false
```

Les autres paramètres de ce fichier sont inchangés.

Fichier `svc-crypto.properties` :

```
#svc-crypto.properties pour responders
KEYSTORE=${jboss.server.home.dir}/conf/svcv2.jks

JTYPE=JKS
ALIAS=svcalias
PASSPHRASE=<motdepasse>
DESTROY=false

#SIGNATURE.ALGO=SHA1withRSA
#ajout d'un fournisseur de signature (option)
CRYPTO.PROVIDER=org.bouncycastle.jce.provider.BouncyCastleProvider

#activation du wrapper (pour SHA1withRSA)
WRAPPEROPENSSL.ACTIVE=false
```

La dernière ligne de ce fichier permet d'activer ou de désactiver l'appel à la signature via OpenSSL :
`WRAPPEROPENSSL.ACTIVE=false` est la configuration nécessaire pour utiliser la signature Java.
`WRAPPEROPENSSL.ACTIVE=true` est la configuration nécessaire pour utiliser la signature OpenSSL.

- Redémarrer JBOSS :

```
# service jboss start
```