

Actualización 5.2.1 para @firma 5.0.1 revisión 05/06

9 de Junio de 2009



JUNTA DE ANDALUCÍA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA



ÍNDICE

1. Novedades
2. Requisitos de la actualización
3. Pasos para la actualización
4. Proceso de actualización
 - I. Determinar opciones de actualización
 - II. Actualizar esquemas de base de datos
 - III. Configuración del CD
 - IV. Lanzamiento de los Scripts
 - V. Copia de las nuevas librerías de IAIK
 - VI. Configuración de @firma 5.2.1
5. Arranque y comprobación del servidor



1. Novedades

a. Nuevas Características

I. Módulo de Firma

- Incluye el formato de firma XAdES en su versión 1.3.2, según la especificación ETSI TS 101 903. Mantiene la compatibilidad con la versión 1.1.1. No soporta la versión 1.2.2
- Validación y generación de firmas electrónicas en formato CAdES-BES/T, soportando las versiones 1.6.3 y v1.7.3.
- Integración con dispositivos HSM nCipher a través de la interfaz PKCS#11.



1. Novedades

a. Nuevas Características

II. Módulo de Validación

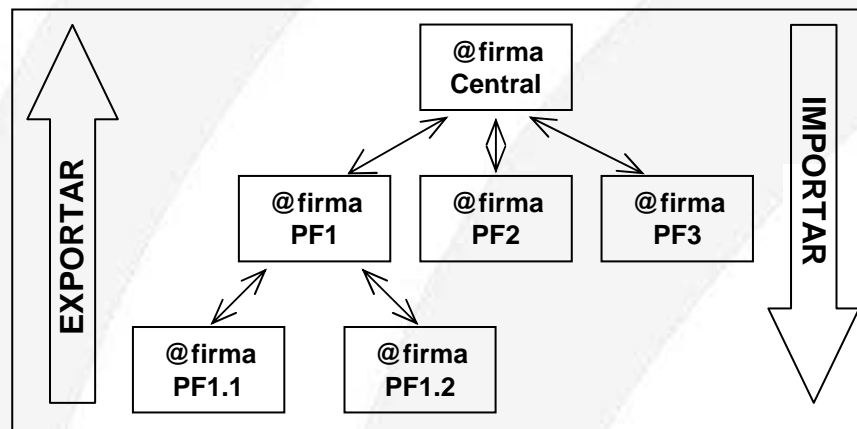
- **Soporta peticiones OCSP firmadas como cliente y como servidor. Podrá servir como OCSP para los prestadores configurados y podrá realizar peticiones hacia servidores OCSP privados como la FNMT.**
- **Se crea una caché de CRLs en memoria (L1), mejorando el rendimiento en la consulta de CRLs. Sirve de apoyo a la caché de nivel 2 (L2) para el almacenamiento de CRLs en BBDD.**
- **Se añade la posibilidad de restringir el uso de los PSCs y sus tipos de certificados a la aplicaciones deseadas.**
- **Se devuelve código 4 como respuesta si no se ha podido comprobar el estado de revocación de un certificado.**

1. Novedades

a. Nuevas Características

III. Módulo de Auditoría

- Se han integrado los módulos de auditoría y monitorización en una única herramienta de usuario; discriminando el acceso a cada funcionalidad en base al perfil del usuario.
- Incluye la posibilidad generar y consultar estadísticas con plataformas federadas.



1. Novedades

a. Nuevas Características

IV. General

- Se ordenan alfabéticamente las aplicaciones y unidades organizativas en la consola de Administración.
- Se añaden nuevas alarmas, entre ellas, alarmas para avisar de incorporaciones y caídas de nodos en el cluster.
- Se mejora el procesador de logs, permitiendo el procesado de archivos mayores.
- Se optimiza el manejo de los campos tipo BLOB, mejorando el rendimiento de la base de datos.

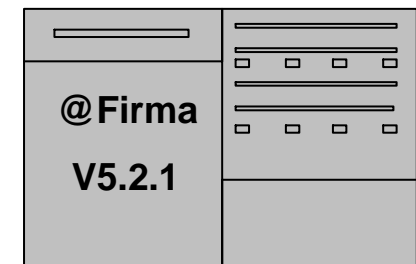
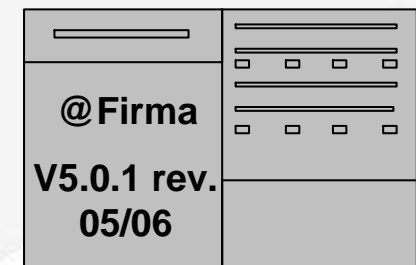
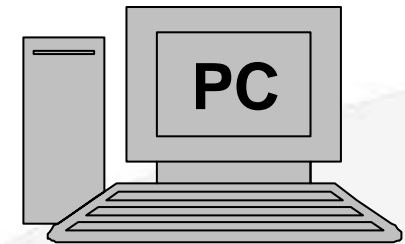
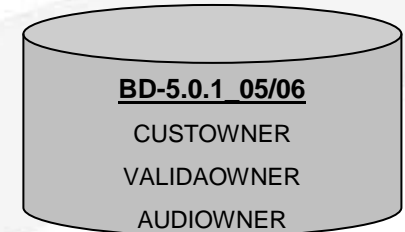


2. Requisitos para la actualización

- a. Tener definidas las variables de entorno JAVA_HOME y JBOSS_HOME.
- b. Tener instalada la herramienta ANT y la variable ANT_HOME.
- c. Tener instalada la versión 5.0.1 de @firma en su revisión 05 ó 06.
 - La actualización no soporta otras versiones.
 - Para otras versiones se debe usar una nueva instalación o actualizar la plataforma hasta una de las versiones soportadas.
- d. Tener correctamente instalados junto a al servidor jBoss de la plataforma, el cliente TSA y el procesador de logs externo.
 - Deben estar en la mismo directorio las carpetas jboss-4.0.2, tsaClient y ProcesaLogsExt.
- e. Tener acceso a las nuevas librerías de IAIK necesarias para la nueva versión 5.2.1:
 - TSA (iaik_tsa.jar, 57KB)
 - XSEC v1.04 build 40 (iaik_xsect.jar, 265KB)
 - XADES v1.3.2_1.01 build 12 (iaik_xades.jar, 168KB)
 - PKCS11Provider v1.2.4 (iaikPkcs11Provider.jar, 343KB)

3. Pasos para la actualización

1. Actualizar los esquemas de base de datos
2. Configurar los archivos del CD antes de la actualización.
3. Actualizar los archivos del servidor @firma, el procesado de logs externo y el cliente de TSA mediante los scripts del CD.
4. Configuración de archivos desplegados tras la actualización.



4. Proceso de actualización

I. Determinar opciones de actualización

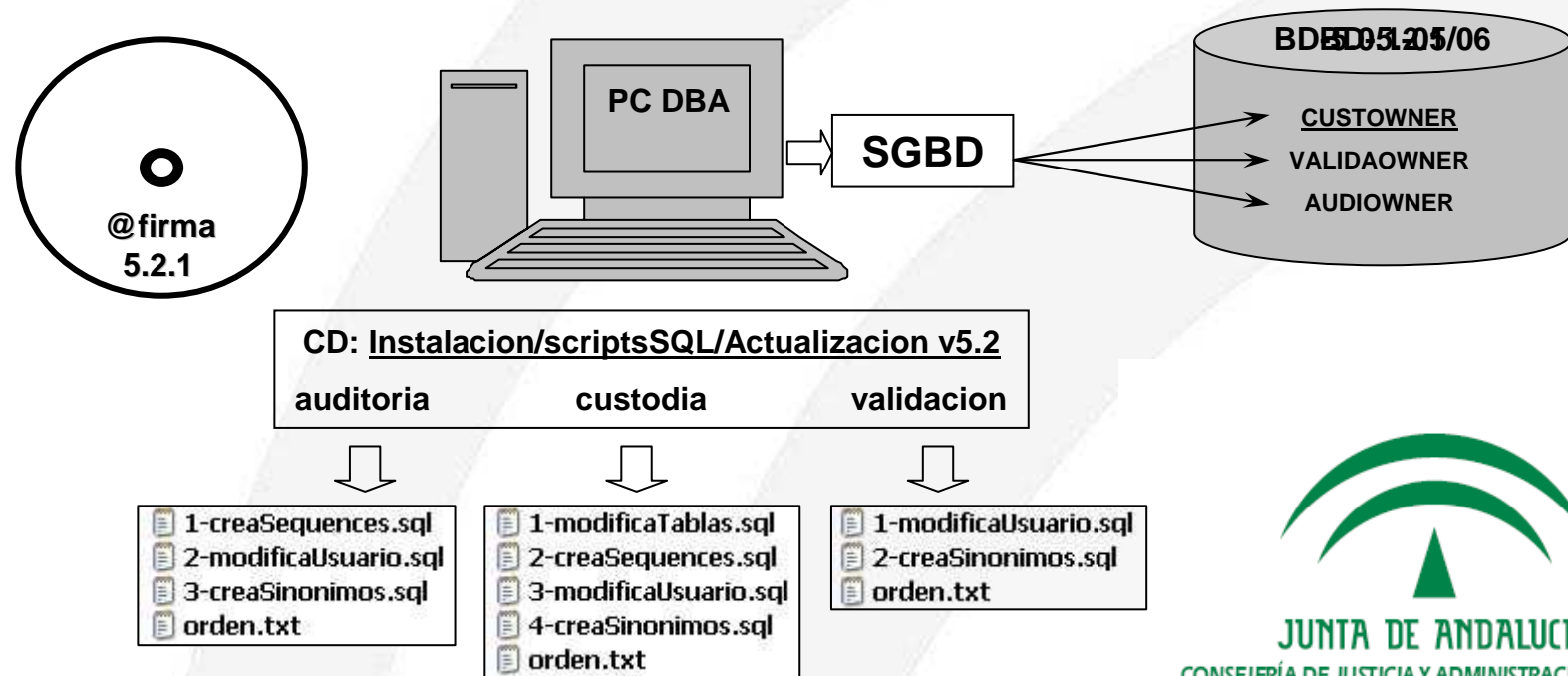
- **El script de actualización disponible en el CD nos ofrece las siguientes posibilidades a la hora de actualizar:**
 - **Actualización con y sin extensión de compatibilidad con @firma 4.**
 - **Usar Keystores PKCS#12 o JCEKS.**
- **Se han detectado problemas en Linux con el tratamiento de los Keystores del tipo PKCS#12, de forma que se recomienda usar JCEKS para actualizar el servidor.**



4. Proceso de actualización

II. Actualizar esquemas de la base de datos

- Es recomendable que la ejecución de los script de actualización de la base de datos sea realizada por un DBA.
- La actualización no afecta a los datos almacenados por otras versiones, de forma que no es necesario ni migrar datos ni parar el servidor.



4. Proceso de actualización

III. Configuración del CD

- **Es recomendable trabajar en un entorno que nos permita utilizar alguna herramienta para edición de textos.**
- **Será necesario modificar algunos archivos originales del CD con la configuración necesaria para los servidores.**
- **Para realizar estas modificaciones se usará el Manual adjunto en el CD**



4. Proceso de actualización

III. Configuración del CD

I. Configuración de IP o nombre de host del contexto web del núcleo

- Archivo **Instalacion/configuracion/server_config.wsdd**
 - a. Se deben modificar todas las entradas del tipo **<parameter name="jndiURL" value="XX.XX.XX.XX"/>**
 - Sustituir las cadenas **XX.XX.XX.XX** por la IP interna del servidor, es decir, la IP o nombre de host de la interfaz de red donde se levanta el servidor.
 - Ej1. **XX.XX.XX.XX** → **afirmav5des01.cjap.junta-andalucia.es**
 - Ej2. **XX.XX.XX.XX** → **10.244..2.53**
 - b. Se deben modificar todas las entradas del tipo **<endpointURL>https://XX.XX.XX.XX/afirmaws/services/</endpointURL>**
 - Sustituir las cadenas **XX.XX.XX.XX** por el dominio de la URL donde se publica el servidor de cara a los usuarios finales. Obsérvese que la URL especificada siempre debe terminar en la cadena **"/afirmaws/services/"**.
 - Ej. **XX.XX.XX.XX** → **ws083.juntadeandalucia.es**
 - c. Entre los puntos a y b deben sustituirse un total de **128** entradas.

4. Proceso de actualización

III. Configuración del CD

II. Configuración de IP o nombre de host del contexto web de la extensión

- Archivo **Instalacion/configuracionExt/server_config.wsdd**
 - a. Se deben modificar todas las entradas del tipo `<parameter name="jndiURL" value="XXX.XXX.XXX.XXX"/>`
 - Sustituir las cadenas `XXX.XXX.XXX.XXX` por la IP interna del servidor, es decir, la IP o nombre de host de la interfaz de red donde se levanta el servidor.
 - Ej1. `XXX.XXX.XXX.XXX` → `afirmav5des01.cjap.junta-andalucia.es`
 - Ej2. `XXX.XXX.XXX.XXX` → `10.244..2.53`
 - b. Se deben modificar todas las entradas del tipo `<endpointURL>https://XXX.XXX.XXX.XXX/axis/services/</endpointURL>`
 - Sustituir las cadenas `XXX.XXX.XXX.XXX` por el dominio de la URL donde se publica el servidor de cara a los usuarios finales. Obsérvese que la URL especificada siempre debe terminar en la cadena `"/axis/services/"`.
 - Ej. `XXX.XXX.XXX.XXX` → `ws083.juntadeandalucia.es`
 - c. Entre los puntos a y b deben sustituirse un total de **18** entradas.

4. Proceso de actualización

III. Configuración del CD

III. Configuración de IP o nombre de host para la consola de Administración

- Archivo **Instalacion/jboss-4.0.2/tiFramework/constantes.xml**
 - a. Se deben modificar las entradas del tipo **<localhost>** y **<127.0.0.1>**
 - Sustituir cada las cadenas por la IP o nombre de host interno del servidor.
 - Ej. **<localhost>** → **afirmav5des01.cjap.junta-andalucia.es**
<127.0.0.1> → **afirmav5des01.cjap.junta-andalucia.es**
 - b. Deben sustituirse un total de **4** entradas.

IV. Configuración de IP o nombre de host donde se publicaran los esquemas XML de los Servicios Web (XSD)

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/traductor.properties**
 - a. Se deben modificar las entradas del tipo **<localhost>**
 - Sustituir las cadenas por la IP o nombre de host interno del servidor.
 - Ej. **<localhost>** → **afirmav5des01.cjap.junta-andalucia.es**
 - b. Debe sustituirse solo **una** entrada.

4. Proceso de actualización

III. Configuración del CD

V. Configuración de IP o nombre de host para la administración de plataformas remotas

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/AdministracionDelegada.PKCS12.properties** si optamos por keystores **PKCS#12**.
- Archivo **Instalacion/jboss-4.0.2/server/all/conf/AdministracionDelegada.JCEKS.properties** si optamos por keystores **JCEKS**.
 - a. Se deben modificar la entrada **<localhost>**
 - Sustituir la cadena **<localhost>** por la IP o nombre de host interno del servidor.
 - Ej. **<localhost>** → **afirmav5des01.cjap.junta-andalucia.es**
 - b. Deben sustituirse solo **una** entrada.

VI. Configuración de rutas de los almacenes y keystores del servidor

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/ACertificadosDAO.PKCS12.properties** si optamos por keystores **PKCS#12**.
- Archivo **Instalacion/jboss-4.0.2/server/all/conf/ACertificadosDAO.JCEKS.properties** si optamos por keystores **JCEKS**.
 - a. Se deben modificar las entradas del tipo **<ruta absoluta JBOSS>**
 - Sustituir la cadenas **<ruta absoluta JBOSS>** por la ruta donde se encuentra alojada la carpeta **jboss-4.0.2**
 - Ej. **<ruta absoluta JBOSS>** → **/export/home/firmaAdmin**
 - b. Deben sustituirse **13** entradas.

4. Proceso de actualización

III. Configuración del CD

VII. Configuración de rutas para el módulo de auditoría del servidor

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/CienteAuditoria.properties.**
 - a. Se deben modificar las entradas del tipo **<ruta absoluta JBOSS>**
 - Sustituir la cadenas **<ruta absoluta JBOSS>** por la ruta donde se encuentra alojada la carpeta **jboss-4.0.2**
 - Ej. **<ruta absoluta JBOSS>** → **/export/home/firmaAdmin**
 - b. Deben sustituirse **2** entradas.

VIII. Configuración de rutas del contexto web del servidor

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/contexto.properties.**
 - a. Se debe modificar la **<ruta absoluta JBOSS>**
 - Sustituir la cadena **<ruta absoluta JBOSS>** por la ruta donde se encuentra alojada la carpeta **jboss-4.0.2**
 - Ej. **<ruta absoluta JBOSS>** → **/export/home/firmaAdmin**
 - b. Deben sustituirse **una** entrada.



4. Proceso de actualización

III. Configuración del CD

IX. Configuración de rutas para la administración delegada de plataformas federadas

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/AdministracionDelegada.PKCS12.properties** si optamos por keystores **PKCS#12**.
- Archivo **Instalacion/jboss-4.0.2/server/all/conf/AdministracionDelegada.JCEKS.properties** si optamos por keystores **JCEKS**.
 - a. Se deben modificar las entradas del tipo **<ruta absoluta JBOSS>**
 - Sustituir la cadenas **<ruta absoluta JBOSS>** por la ruta donde se encuentra alojada la carpeta **jboss-4.0.2**
 - Ej. **<ruta absoluta JBOSS>** → **/export/home/firmaAdmin**
 - b. Deben sustituirse **2** entradas.

X. Configuración del funcionamiento de los métodos de validación

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/validacion.properties**
 - a. Configurar la propiedad **validarConformeRFC3280** con los valores posibles *true* o *false*, según se desee o no validar las firmas conforme a la RFC3280. Debe configurarse a la **false** para poder usar cierto tipo de certificados, de forma que se recomienda este valor.
 - b. Configurar la propiedad **hayQueActualizar** a **true** para que la plataforma realice ciertos cambios en la configuración durante el primer arranque de la versión 5.2.1.
 - c. Configurar **canonicalizarIds** a **false**, de forma que tras el primer arranque, la plataforma lo reconfigurará a **true**.
 - d. Configurar **conexion.httpClient** a *true* para usar la librería de Jakarta para conexiones HTTP o *false* para usar los métodos nativos de Java. (Recomendado **true**)
 - e. Configurar **conexion.IdapNovell** a *true* para usar la librería de Novell para conexiones LDAP o *false* para usar los métodos nativos de Java. (Recomendado **true**)

4. Proceso de actualización

III. Configuración del CD

XI. Configuración del certificado de firma del sistema

- **Instalacion/jboss-4.0.2/server/all/conf/mfirma/aliasServerCert.properties**
- Este archivo define el *alias* del certificado que usará el servidor para firmas del sistema. Debe configurarse con uno de los alias contenidos en el keystore **CertificadosSistema**, al cual podemos acceder desde la herramienta de Administración en la sección de gestión de keystores y contraseñas.
- El alias usado por defecto es **default**, pero es necesario revisar que efectivamente ese alias existe en el keystore mencionado para evitar errores a la hora de firmar los justificantes de firma.



4. Proceso de actualización

III. Configuración del CD

XII. Configuración del proxy

- Archivo **Instalacion/jboss-4.0.2/server/all/conf/proxy.properties**
 - a. Configurar la propiedad **proxy.operational**
 - **NONE** → No se emplea configuración de proxy
 - **NONE_AUTHENTICATION** → Se usa proxy sin autenticación
 - **BASIC_AUTHENTICATION** → Se usa proxy con autenticación básica
 - **NTLM_AUTHENTICATION** → Se emplea proxy con autenticación NTLM
 - b. Configurar la propiedad **proxy.ip** con la IP o nombre de host del proxy.
 - c. Configurar la propiedad **proxy.port** con la puerto configurado en el proxy.
 - d. Configurar la propiedad **proxy.user.name** con el nombre de usuario para autenticación básica o NTLM.
 - e. Configurar la propiedad **proxy.user.password** con el password para autenticación básica o NTLM.
 - f. Configurar la propiedad **proxy.domain** con el dominio para autenticación NTLM.
 - g. Configurar la propiedad **check.local.address** para rutas locales.
 - **true** → Se usará conexión a través del proxy para rutas locales.
 - **false** → Conectará sin pasar el proxy para rutas locales. (Recomendado)

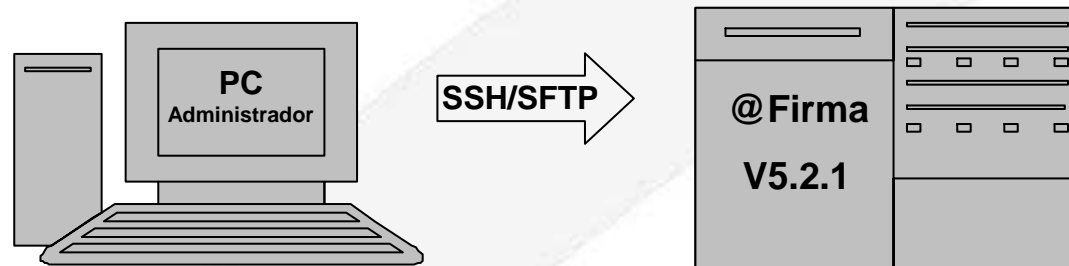
4. Proceso de actualización

IV. Lanzamiento de scripts de actualización

- El script **actualizacion_5.0.1-5.2.1.sh** actualizará el núcleo de @firma de la versión 5.0.1_05/06 a la versión 5.2.1, adecuando si se usa la opción, la extensión de compatibilidad con @firma 4.
- El proceso de actualización genera automáticamente una copia de seguridad de los archivos modificados, de forma que se podrá restaurar la versión 5.0.1 en cualquier momento tras la actualización.
- En caso de error de actualización, el script restaura automáticamente la versión 5.0.1, mostrando el motivo del error en la salida del comando.
- Para restaurar manualmente la versión 5.0.1_05/06 se usa el siguiente comando:
 - `~# sh restaura_5.0.1.sh <directorio_del_servidor_a_restaurar>
<directorio_de_la_copia_de_seguridad>`
 - Ejemplo:
`~# sh restaura_5.0.1.sh /export/home/firmaAdmin
/export/home/firmaAdmin/backup/afirma_backup_09-06-09_12-00-00`

4. Proceso de actualización

IV. Lanzamiento de Scripts



Pasar el comando dos2unix y dar permisos de ejecución a los scripts de actualización y restauración:

SOLARIS

```
~ # dos2unix actualizacion_5.0.1-5.2.1.sh actualizacion_5.0.1-5.2.1.sh
~ # dos2unix restaura_5.0.1.sh restaura_5.0.1.sh
~ # chmod +x actualizacion_5.0.1-5.2.1.sh
~ # chmod +x restaura_5.0.1.sh
```

LINUX

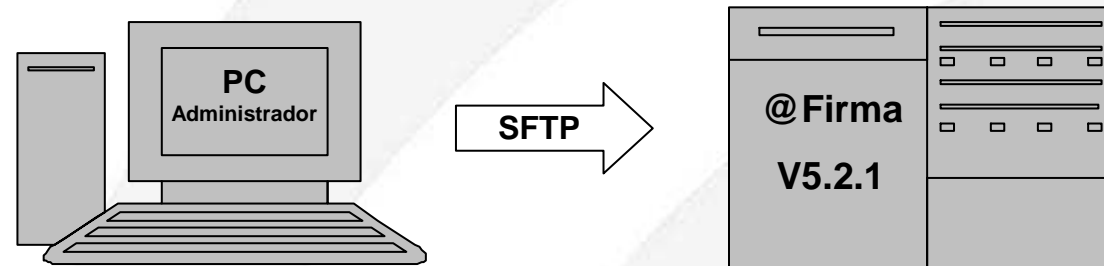
```
~ # dos2unix actualizacion_5.0.1-5.2.1.sh
~ # dos2unix restaura_5.0.1.sh
~ # chmod +x actualizacion_5.0.1-5.2.1.sh
~ # chmod +x restaura_5.0.1.sh
```

4. Proceso de actualización

V. Copia de las nuevas librerías de IAIK

- La versión 5.2.1 de @firma necesita nuevas librerías de IAIK, las cuales serán públicas como descarga privada para los organismos de la Junta de Andalucía en el portal de Administración Electrónica:

<https://ws024.juntadeandalucia.es/pluton/index.jsp>



Copiar las nuevas librerías de IAIK



filezilla



- iaikPkcs11Provider.jar
- iaik_xades.jar
- iaik_xsect.jar
- iaik_tsa.jar

/export/home/firmaAdmin/jboss-4.0.2/server/all/lib

4. Proceso de actualización

VI. Configuración de @firma 5.2.1

- Para no perder la configuración ya existente en la versión 5.0.1_05/06 es necesario realizar algunos cambios a mano en los archivos del servidor.
- Como en la configuración del CD, es recomendable hacer uso de una herramienta de edición de textos para este proceso de configuración.



Descargar archivos



filezilla

`/export/home/firmaAdmin/`

`jboss-4.0.2/server/all/conf/configuracionArrobaFirma5_0.xml` (Núcleo)
`jboss-4.0.2/server/all/deploy/cluster-service.xml` (Núcleo)
`ProcesaLogsExt/conf/hibernate.procesarlog.cfg.xml` (ProcesaLogs)
`tsaClient/conf/clienteTSAConf.properties` (Cliente TSA)
`jboss-4.0.2/server/all/conf/jndiMigration.properties` (Extensión)
`jboss-4.0.2/server/all/deploy/afirma-webAuth-service.xml` (Aut. Web)

4. Proceso de actualización

VI. Configuración de @firma 5.2.1

I. Archivo configuracionArrobaFirma5_0.xml

1. Buscar la cadena “**centroConfiguracionServidorOCSP**”. Una vez encontrada, se deben incluir los siguientes elementos al mismo nivel que el elemento **<algoritmosHashAceptados>**.

```
<algoritmosFirmaAceptados>
<tiDatosAlgoritmo>
<oidAlgoritmoFirma>1.2.840.113549.1.1.5</oidAlgoritmoFirma>
<nombre>SHA1WithRSAEncryption</nombre>
</tiDatosAlgoritmo>
<tiDatosAlgoritmo>
<oidAlgoritmoFirma>1.2.840.113549.1.1.11</oidAlgoritmoFirma>
<nombre>SHA256WithRSAEncryption</nombre>
</tiDatosAlgoritmo>
<tiDatosAlgoritmo>
<oidAlgoritmoFirma>1.2.840.113549.1.1.12</oidAlgoritmoFirma>
<nombre>SHA384WithRSAEncryption</nombre>
</tiDatosAlgoritmo>
<tiDatosAlgoritmo>
<oidAlgoritmoFirma>1.2.840.113549.1.1.13</oidAlgoritmoFirma>
<nombre>SHA512WithRSAEncryption</nombre>
</tiDatosAlgoritmo>
</algoritmosFirmaAceptados>
```


4. Proceso de actualización

VI. Configuración de @firma 5.2.1

I. Archivo configuracionArrobaFirma5_0.xml

2. Buscar la cadena “**contrasenyas**”. Una vez encontrada, se deben incluir los dos nuevos elementos de entrada (**<entry>**) al mismo nivel que los demás, como hijos del elemento **<parametros>**.

- Las contraseñas incluidas no deben ser modificadas. De hacerlo el servidor no arrancará correctamente.

```
<entry>
<string>repositorio.contrasenya.AlmacenConfianzaPF</string>
<char-array>changeit</char-array>
</entry>
<entry>
<string>repositorio.contrasenya.KeystoreClienteOCSP</string>
<char-array>topSecret</char-array>
</entry>
```



4. Proceso de actualización

VI. Configuración de @firma 5.2.1

II. Archivo cluster-service.xml

- La nueva versión de la plataforma solo usa una partición para el cluster de jBoss, de forma que será necesario eliminar la partición **AFirma5-Partition** de la versión 5.0.1 y reconfigurar los **DataSource**
 1. Se **elimina** el elemento **<mbean>** y todo su contenido correspondiente a la partición **AFirma5-Partition**.

```
<mbean code="org.jboss.ha.framework.server.ClusterPartition"
name="jboss:service=AFirma5-Partition">
....
</mbean>
```

2. Se **sustituyen** todas las cadenas **AFirma5-Partition** por **DefaultPartition**, sustituyendo un total de **6 cadenas más el número de DataSources**.
3. Se comprueba la configuración de red de la partición **DefaultPartition**, usando la misma IP y puerto para los paquetes UDP en todos los miembros del cluster.

```
....
<UDP mcast_addr="XX.XX.XX.XX" mcast_port="XXXXXX"
bind_addr="IP_HOST_SERVIDOR" ip_mcast="true"
....
```

4. Proceso de actualización

VI. Configuración de @firma 5.2.1

III. Archivo hibernate.procesarlog.cfg.xml

- En este archivo se configura la conexión al esquema de base de datos de auditoría. Las propiedades en rojo deben ser configuradas según la conexión a la base de datos.

```
<property name="hibernate.connection.driver_class">  
oracle.jdbc.driver.OracleDriver  
</property>  
<property name="hibernate.connection.url">  
jdbc:oracle:oci:@IP_BBDD:PUERTO:SID_BD  
</property>  
<property name="hibernate.transaction.factory_class">  
org.hibernate.transaction.JDBCTransactionFactory</property>  
<property name="dialect">  
org.hibernate.dialect.Oracle9Dialect  
</property>  
<property name="hibernate.connection.username">  
USUARIO_BD  
</property>  
<property name="hibernate.connection.password">  
PASSWORD_BD  
</property>
```



4. Proceso de actualización

VI. Configuración de @firma 5.2.1

IV. Archivo clienteTSAConf.properties

- Se añade una nueva propiedad para definir el modo de conexión con el servidor de sello de tiempo (TSA).
- Esta configuración no es necesaria para el notario electrónico, pero sí para el funcionamiento del cliente TSA.

Modo de conexión. Valores posibles: WS o RFC.

WS (valor por defecto): Se generará una petición WS típica de la TSA

de @firma (SOAP-SEC).

RFC: Se generará una petición TimeStampRequest, y se aceptará

únicamente respuestas TimeStampResponse, tal y como se indica

en la RFC.

modoConexion = WS



4. Proceso de actualización

VI. Configuración de @firma 5.2.1

V. Archivo jndiMigration.properties

- Cambiar la partición configurada para la extensión de compatibilidad con @firma 4.
- Se sustituye en el archivo la cadena **AFirma5-Partition** por **DefaultPartition**

VI. Archivo afirmas-webAuth-service.xml

- Solo encontraremos este archivo en el caso de tener instalado el componente de Autenticación Web mediante Tickets de @firma5.
- Se sustituyen en el archivo las cadenas **AFirma5-Partition** por **DefaultPartition**, sustituyendo un total de dos entradas.
- Después de modificar este archivo es necesario modificar el contenido del contexto web de este componente:
 - a. Abrir el archivo **jboss-4.0.2/server/all/deploy/webAuthentication.ear** como un archivo ZIP.
 - b. Eliminar las siguientes librerías contenidas en la ruta **authentication.war\WEB-INF\lib**:
 - axis.jar**, **wss4j.jar** y **commons-logging.jar** en cualquiera de sus versiones.



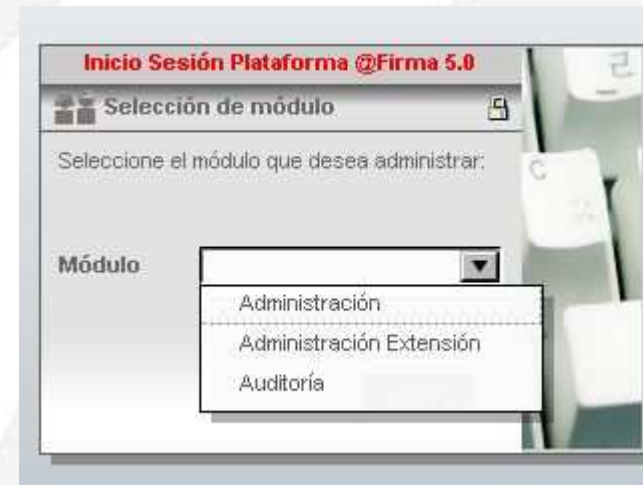
5. Arranque y comprobación del servidor

- Arranque del servidor
 - Una vez configurado el servidor ya podemos arrancarlo. Podemos usar el servicio configurado en el sistema o ejecutando el siguiente comando como **root**:
 - **~# sh /export/home/firmaAdmin/jboss-4.0.2/bin/run.sh &**
 - Para comprobar el proceso de arranque revisamos el archivo **server.log**:
 - **~# less /export/home/firmaAdmin/jboss-4.0.2/server/all/log/server.log**
 - **Tras el comando SHIFT+F (tail del fichero)**
- Comprobación del servidor
 - Una vez terminado el arranque podremos comprobar el funcionamiento y los cambios realizados durante la actualización.
 1. **El primer paso es abrir la consola de administración y auditoría usando un Navegador.**
 2. **Después comprobamos que se han publicado los servicios correctamente.**





5. Arranque y comprobación del servidor

1. Comprobación de la consola de Administración y Auditoría
 - **Abrir la consola usando la siguiente URL:**
 - `https://<nombre de host o IP del servidor>/Consola`
 - Ejemplo. <https://afirmav5des05.cjap.junta-andalucia.es/Consola>
 - **Se abrirá una página como la siguiente.**
 - Se observa que aparecen los siguientes componentes de configuración, según sea un servidor con o sin extensión.



5. Arranque y comprobación del servidor

1. Comprobación de la consola de Administración y Auditoría
 - **Entrando en el componente de Administración**
 - La consola de Administración se correspondiente con la versión 5.2.1 y debe incluir dos secciones nuevas. La gestión de plataformas federadas  y la gestión de OCSP .
 - Gestión de Plataforma Federadas



- Plataformas federadas tras inicializar la configuración



5. Arranque y comprobación del servidor

1. Comprobación de la consola de Administración y Auditoría
 - **Entrando en el componente de Administración**
 - Gestión de OCSP

Módulo de administración

Gestión de OCSP

Algoritmo de Hash: SHA1

Algoritmo de Firma: SHA1WithRSAEncryption

Identificador certificado defecto:

RequestorName Obligatorio

Modificar

SHA1WithRSAEncryption

SHA256WithRSAEncryption

SHA384WithRSAEncryption

SHA512WithRSAEncryption

- Gestión de Alarmas
 - Deben aparecer las alarmas de la 0-20 y de la 22-25 (**no debe aparecer la alarma 21**).

5. Arranque y comprobación del servidor

2. Comprobación de los servicios publicados

- **Comprobación de los servicios del núcleo de @firma**
 - `https://<nombre de host o IP del servidor>/afirmaws/services/AxisServlet`
 - Ejemplo,
`https://afirmav5des05.cjap.junta-andalucia.es/afirmaws/services/AxisServlet`



5. Arranque y comprobación del servidor

2. Comprobación de los servicios publicados

- **Comprobación de los servicios de la extensión**
 - **Será necesario introducir nombre de usuario y contraseña**
 - `https://<nombre de host o IP del servidor>/axis/services/AxisServlet`
 - Ejemplo,
`https://afirmav5des05.cjap.junta-andalucia.es/axis/services/AxisServlet`



5. Arranque y comprobación del servidor

2. Comprobación de los servicios publicados

- **Comprobación de los servicios del componente de Autenticación**
 - `https://<nombre de host o IP del servidor>/authentication/servlet/AxisServlet`
 - Ejemplo,
`https://afirmav5des05.cjap.junta-andalucia.es/authentication/servlet/AxisServlet`

