



Servicio de WebSSO

Manual de instalación y configuración

Versión: 1.1

[Versión del Producto]

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de la Junta de Andalucía.



Servicio de WebSSO
Manual de instalación y configuración

**Consejería de Economía,
Innovación y Ciencia**

HOJA DE CONTROL

| | | | |
|---------------------|-----------------------|----------------------------|------------|
| Organismo | Innovación y Ciencia | | |
| Proyecto | Servicio de WebSSO | | |
| Entregable | Manual de instalación | | |
| Autor | SIA | | |
| Aprobado por | | Fecha Aprobación | DD/MM/AAAA |
| | | Nº Total de Páginas | 80 |

REGISTRO DE CAMBIOS

| Versión | Causa del Cambio | Responsable del Cambio | Fecha del Cambio |
|----------------|-------------------------|-------------------------------|-------------------------|
| 0100 | Versión inicial | <Nombre Apellido1 Apellido2> | DD/MM/AAAA |
| 1.1 | | SANDETEL | |
| | | | |

CONTROL DE DISTRIBUCIÓN

| Nombre y Apellidos |
|------------------------------|
| <Nombre Apellido1 Apellido2> |
| |
| |
| |
| |

ÍNDICE

| | | |
|----------|--|-----------|
| 1 | Introducción..... | 5 |
| 1.1 | Objeto..... | 5 |
| 1.2 | Alcance..... | 5 |
| 1.3 | Glosario y definiciones..... | 5 |
| 1.4 | Recursos adicionales..... | 5 |
| 2 | Requisitos técnicos para la implantación..... | 6 |
| 2.1 | Materiales..... | 6 |
| 2.1.1 | Sistemas..... | 6 |
| 2.1.2 | Comunicaciones..... | 6 |
| 2.1.3 | Seguridad..... | 7 |
| 2.2 | Organizativos..... | 7 |
| 3 | Arquitectura..... | 8 |
| 4 | Instalación del software base..... | 9 |
| 4.1 | Creación del usuario y grupo “openam” | 9 |
| 4.2 | Instalación de la máquina virtual Java (JRE)..... | 9 |
| 4.3 | Instalación del servidor de aplicaciones | 10 |
| 4.3.1 | Instalación de “Apache Tomcat” | 10 |
| 4.3.2 | Configuración de SSL..... | 12 |
| 4.3.3 | Configuración de los parámetros de arranque del servidor de aplicaciones.... | 15 |
| 4.4 | Configuración del desplegable..... | 16 |
| 4.4.1 | Compilación del módulo..... | 16 |
| 4.4.2 | Personalización páginas del SSOWeb para cada entorno/dominio..... | 16 |
| 4.4.3 | Configuración Applet @Firma y Conexión con @Firma..... | 18 |
| 4.5 | Despliegue de la aplicación..... | 19 |
| 5 | Servidor primario de OpenAM | 20 |
| 5.1 | Configuración de la instancia principal de OpenAM..... | 20 |
| 5.2 | Configuración de los dominios GUIA y correo..... | 26 |
| 5.2.1 | Instalación Administration Tools..... | 26 |
| 5.2.2 | Registro del módulo de autenticación Afirma en Openam..... | 28 |
| 5.2.3 | Configuración dominio correo..... | 29 |
| 5.2.3.1 | Crear el dominio..... | 29 |

| | |
|--|----|
| 5.2.3.2 Crear y configurar el DataStore..... | 29 |
| 5.2.3.3 Configuración del procedimiento de Autenticación..... | 33 |
| 5.2.4 Configuración dominio GUIA..... | 37 |
| 5.2.4.1 Crear el dominio..... | 37 |
| 5.2.4.2 Crear y configurar el DataStore..... | 37 |
| 5.2.4.3 Configuración del procedimiento de Autenticación..... | 40 |
| 5.2.5 Verificación de la instalación..... | 43 |
| 5.3 Creación de los IDPs..... | 48 |
| 5.3.1 Configuración del certificado para el IDP..... | 48 |
| 5.3.2 Creación del IPD para el dominio de correo..... | 49 |
| 5.3.3 Creación del IPD para el dominio GUIA..... | 54 |
| 6 Servidores Secundarios de OpenAM..... | 57 |
| 7 Configuración del clúster de OpenAM..... | 66 |
| 7.1 Añadir nodos secundarios al cluster..... | 66 |
| 7.2 Instalación del balanceador de sesiones..... | 68 |
| 7.3 Configuración del balanceo de sesiones en OpenAM..... | 72 |
| 8 Anexos..... | 75 |
| 8.1 Depuración de errores..... | 75 |
| 8.2 Mapeador de Atributos JDAIDPAttributeMapper..... | 76 |
| 8.3 Página de Verificación del componente de autenticación por certificados..... | 78 |
| 8.4 Urls..... | 79 |

1 Introducción

1.1 Objeto

En el presente documento se describe el procedimiento de instalación y configuración del proyecto SSOWeb de la Junta de Andalucía. El documento recoge el despliegue en cluster de su servidor de aplicaciones, una versión adaptada del producto OpenAm v10.0 de ForgeRock, además de los pasos de configuración necesarios para cubrir los requisitos de funcionales establecidos en el proyecto, en concreto su integración con el repositorio de Identidades GUIA y el Ldap de correo corporativo.

1.2 Alcance

El documento va dirigido a personal técnico encargado de la instalación y configuración del SSOWeb.

1.3 Glosario y definiciones

- SSO (Single Sign On). Es un mecanismo de autenticación mediante el cuál el usuario se autentica una vez propagando la identidad a las aplicaciones
- SAML. Es un estándar basado en XML para el intercambio de mensajes de autenticación y autorización entre dominios de seguridad.
- Federación de Identidades. La identidad federada es una de las soluciones para abordar la gestión de identidad en los sistemas de información. Su objetivo es obtener una gestión de usuarios eficiente, la sincronización de los datos identificativos, gestión de acceso, servicios de agrupación, servicios de directorio, auditoria e informes
- SP (Service Provider). Es el elemento que consume la información de autenticación y autorización en la relación federada. Se puede equiparar a la aplicación de negocio a integrar.
- IDP (IDentity Provider). Es el elemento que contiene la información de origen de la identidad en una relación federada.

1.4 Recursos adicionales

- Documentación oficial de ForgeRock para la instalación de OpenAm: <https://wikis.forgerock.org/confluence/display/openam/OpenAM+Documentation>
- Plan de pruebas: JdA - WebSSO - Documento de pruebas v1.0.odt

2 Requisitos técnicos para la implantación

2.1 Materiales

2.1.1 Sistemas

La instalación del software puede realizarse sobre sistemas virtualizados o físicos. En cualquier caso los requisitos son los siguientes:

- Dos servidores RedHat Linux versión 5.3./5.4 64 bits con las siguientes características:
 - Mínimas:
 - 2 Gb de RAM.
 - Multinúcleo: 1 núcleos.
 - 1 tarjeta de red.
 - Espacio de 6 GB
 - Recomendables:
 - 6 Gb de RAM.
 - Multinúcleo: 4 nucleos.
 - Dos tarjetas de red.
 - Espacio de 120 GB
- Los dos servidores deberán disponer de este software base (en este documento se describirá el proceso de instalación de estos componentes):
 - Maquina virtual java 1.6.X de 64 bits.
 - Apache Tomcat 6.X para sistemas Linux
- Sistemas externos:
 - Repositorio LDAP GUIA.
 - Repositorio LDAP de correo corporativo JdA.
 - Servidor de @firma v5.
- Sincronización NTP de todos los servidores de la infraestructura (servidores del IdP, servidores de los SP)

2.1.2 Comunicaciones

- **Enlaces de alta velocidad para las tarjetas de red.**
- **Configuración de Firewalls:** conectividad entre los servidores de

OpenAm, Guía y Correo Corporativo. Conectividad al puerto HTTP a los servidores de OpenAm. Conectividad desde los servidores de OpenAm con @firma (Core).

- **Balanceadores de carga:** para el reparto de carga se utilizará una IP de servicio que balanceará las peticiones entre los dos nodos de manera transparente.
- **Proxies:** se debe evitar la reescritura de nombres en los componentes de la infraestructura.

2.1.3 Seguridad

- Será necesario disponer de un certificado digital para la publicación por HTTPs dentro de los servidores de aplicaciones del proyecto.
- También será necesario un certificado digital para la firma de los mensajes SAMLs generados por el IDP.

2.2 Organizativos

- Cuenta de servidor en GUIA para la aplicación SSOWeb. La cuenta debe tener privilegios de lectura sobre todo el directorio. Nota: no se requieren ni se recomiendan permisos de escritura para estas cuentas.
- Cuenta de aplicación en el Ldap de correo corporativo con permisos de lectura sobre todo el directorio y todos los atributos. Nota: no se requieren ni se recomiendan permisos de escritura para estas cuentas.
- Se deberá integrar los servicios de OpenAm en la infraestructura de monitorización.
- Se deberá integrar los nuevos servidores de OpenAm dentro de la infraestructura de backup.
- Grupo encargado de gestionar las peticiones para la nueva infraestructura.
- Alta en DNS para el cluster de SSOWeb, alta también en dns para los nombres de los cada uno de los nodos del cluster. Nota: el alta del DNS de los nodos puede ser sustituido por alta en los hosts de cada máquina, aunque el producto recomienda el alta directamente en los dns para entornos de producción.

3 Arquitectura

En la ilustración que sigue se muestra la arquitectura completa del SSOWeb.

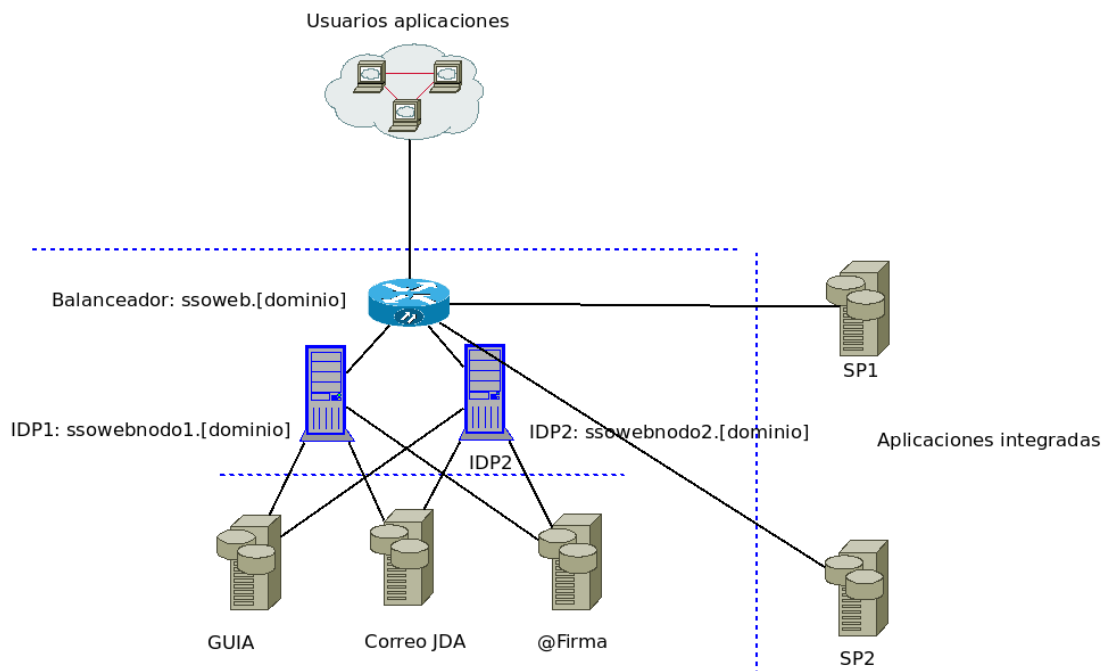


Figura 1. Arquitectura

Los servidores de OpenAM (IDPs) se encuentran desplegados en alta disponibilidad mediante un balanceador de red. El balanceador gestiona el nombre de dominio para todo el cluster y redirige las peticiones hacia los nodos finales. Las funcionalidades del producto como SSO no requieren que el balanceador este en modo sticky, aunque es recomendable, ya que el software está preparado para detectar si la sesión de usuario está activa en el nodo y si no, redirigir las peticiones al nodo adecuado. No sucede lo mismo con la consola web de administración del producto (/opensso/console), para la cual se recomienda activar algún modo sticky en el balanceo.

El producto requiere que cada nodo tenga su propio FQDN, distinto del asignado al balanceador, para permitir las comunicaciones directas entre los nodos. Si no se desea dar de alta estos en el DNS, se pueden dar de alta los localmente en cada máquina a través del fichero host, aunque esto no es recomendable para entornos de producción.

El proyecto de SSOWeb se integra con el repositorio de identidades GUIA (OID u OVD) y el Idap del correo corporativo. Además, el proyecto hace uso de un



Servicio de WebSSO
Manual de instalación y configuración

**Consejería de Economía,
Innovación y Ciencia**

servidor @firma para la validación de las firmas y los certificados de usuario capturados en los procedimientos de Login por certificado digital.

Las aplicaciones integradas dentro del SSO se denominan SP (Service Providers).

4 Instalación del software base

4.1 Creación del usuario y grupo “openam”

Se recomienda que la configuración y arranque de los servidores de aplicaciones se realice con un usuario de sistema específico para el proyecto, por ejemplo “openam.”

A continuación se incluye, a modo ilustrativo, la creación de este usuario bajo un sistema linux.

```
[root@server1 tmp] groupadd openam
[root@server1 tmp] useradd -d /home/openam/ -g openam -s /bin/bash openam
[root@server1 tmp] passwd openam
Changing password for user openam2.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Para verificar que tanto el grupo como el usuario se han creado correctamente, verificar los ficheros **/etc/group** y **/etc/passwd**. Tienen que aparecer la entrada correspondiente al grupo y al usuario (el GID y el UID pueden variar en la máquina destino).

```
[root@server1 tmp] more /etc/group
[...]
openam:x:600:

[root@server1 tmp] more /etc/passwd
[...]
openam:x:600:600::/home/openam:/bin/bash
```

Repetir los pasos anteriores en el segundo servidor Linux.

4.2 Instalación de la máquina virtual Java (JRE)

OpenAM requiere una máquina virtual Java para su ejecución. En este apartado, se detalla un ejemplo de instalación de la misma.

1. Descargar la máquina virtual Java versión “1.6.X” (64 bits) de la página

web de Oracle del siguiente enlace
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

2. Copiar el fichero “**jdk-6.X-linux-x64.bin**” en cada una de las máquinas Linux donde se va a desplegar OpenAM. El directorio donde debe copiarse el fichero de instalación es el directorio en el que se instalan las aplicaciones, por ejemplo: **/opt/software/**
3. Iniciar sesión con usuario **root** en la máquina donde se ha copiado el fichero de instalación del JRE, y cambiar al fichero los permisos de ejecución con el siguiente comando:

```
[root@server1 software] chmod 755 /opt/software/jdk-6.X-linux-x64.bin
```

4. Posicionarse en el directorio donde se ha copiado el fichero del JRE, y ejecutar el siguiente comando para instalarlo:

```
[root@server1 software] ./jdk-6.X-linux-x64.bin
```

5. Se descomprimirá automáticamente el paquete de instalación en el directorio actual de trabajo, creándose el subdirectorio **jdk1.6.X/**
6. Al final de la instalación de los ficheros, pulsar ENTER:

Press Enter to continue . . . Done

7. Cambiar el propietario del directorio del JRE al usuario **openam**

```
[root@server1 software] chown -R openam:openam /opt/software/jdk1.6.X
```

8. Una vez instalado el JRE, eliminar el fichero “**jdk-6.X-linux-x64.bin**” del directorio donde se copió.
9. Repetir los pasos anteriores en el segundo servidor Linux.

4.3 Instalación del servidor de aplicaciones

OpenAM necesita un servidor de aplicaciones para su funcionamiento. El producto es compatible con varios servidores de aplicaciones y versiones de los mismos, aunque en esta guía sólo se contempla un ejemplo de instalación bajo servidor de aplicaciones Tomcat v6.X. Para una instalación bajo otro servidor de aplicaciones o versión se recomienda hacer uso de la documentación oficial del producto: <http://docs.forgerock.org/en/index.html?product=openam&version=10.0.1>

4.3.1 Instalación de “Apache Tomcat”

Para instalar Tomcat v6.X se seguirán estos pasos:

1. Acceder a la web de Apache Tomcat y descargar la versión 6.X para Linux:

<http://archive.apache.org/dist/tomcat/tomcat-6/v6.X.Y/bin/>

2. Copiar el fichero de instalación de Apache Tomcat en el directorio del servidor Linux donde se va a instalar OpenAM, por ejemplo, **/opt/software/**
3. Con usuario **root**, posicionarse en el directorio donde se ha copiado el fichero (por ejemplo **/opt/software**), y extraer el archivo zip con el comando '**unzip**', a continuación renombrar el directorio a **tomcat** :

```
[root@server1 software] unzip apache-tomcat-6.X.zip  
[root@server1 software] mv apache-tomcat-6.X tomcat
```

4. Una vez instalado Tomcat, eliminar el fichero "**apache-tomcat-6.X.zip**" del directorio **/opt/software**, con el comando "**rm**" de Linux.
5. Cambiar el propietario del directorio tomcat a **openam**, y modificar los permisos de los archivos con extensión **.sh** que se encuentren en el directorio "**bin**":

```
[root@server1 software] cd /opt/software/  
[root@server1 software] chown -R openam:openam tomcat/  
[root@server1 bin] su - openam  
[openam@server1 software] cd /opt/software/tomcat/bin  
[openam@server1 bin] chmod 750 *
```

6. Posicionarse con usuario **openam** en el directorio de binarios de Tomcat (por ejemplo **/opt/software/tomcat/bin**) y editar los ficheros **startup.sh** y **shutdown.sh**, añadiendo las siguientes líneas al comienzo del fichero:

startup.sh

```
export JAVA_HOME=/opt/software/jdk1.6.X  
export JAVA_OPTS="-Xmx2048M -XX:MaxPermSize=256M"
```

shutdown.sh

```
export JAVA_HOME=/opt/software/jdk1.6.X
```

7. Añadir también al fichero startup.sh la propiedad **-Dfile.encoding=ISO-8859-1** al final de la cadena que comienza por "**export JAVA_OPTS=**"
8. Con el usuario **openam**, posicionarse en el subdirectorio **bin/** de la instalación de Tomcat, y arrancar Tomcat:

```
[openam@descorss01 bin]$ ./startup.sh  
  
Using CATALINA_BASE: /opt/software/tomcat
```

```
Using CATALINA_HOME: /opt/software/tomcat
Using CATALINA_TMPDIR: /opt/software/tomcat/temp
Using JRE_HOME: /opt/software/jdk1.6.X
Using CLASSPATH: /opt/software/tomcat/bin/bootstrap.jar
```

9. Validar el arranque de Tomcat mediante la verificación del fichero de log **\$TOMCAT/logs/catalina.out**. No deben mostrarse errores en el arranque, y debe terminar con la línea **"INFO: Server startup in xxxx ms"**:

```
[openam@descorso01 bin]$ tail-f ../logs/catalina.out

09-abr-2012 19:24:29 org.apache.coyote.http11.Http11Protocol init
INFO: Inicializando Coyote HTTP/1.1 en puerto http-8080
09-abr-2012 19:24:29 org.apache.catalina.startup.Catalina load
INFO: Initialization processed in 810 ms
09-abr-2012 19:24:29 org.apache.catalina.core.StandardService start
INFO: Arrancando servicio Catalina
09-abr-2012 19:24:29 org.apache.catalina.core.StandardEngine start
INFO: Starting Servlet Engine: Apache Tomcat/6.0.33
09-abr-2012 19:24:29 org.apache.catalina.startup.HostConfig deployDirectory
INFO: Despliegue del directorio ROOT de la aplicación web
09-abr-2012 19:24:29 org.apache.catalina.startup.HostConfig deployDirectory
INFO: Despliegue del directorio manager de la aplicación web
09-abr-2012 19:24:29 org.apache.catalina.startup.HostConfig deployDirectory
INFO: Despliegue del directorio examples de la aplicación web
09-abr-2012 19:24:30 org.apache.catalina.startup.HostConfig deployDirectory
INFO: Despliegue del directorio docs de la aplicación web
09-abr-2012 19:24:30 org.apache.catalina.startup.HostConfig deployDirectory
INFO: Despliegue del directorio host-manager de la aplicación web
09-abr-2012 19:24:30 org.apache.coyote.http11.Http11Protocol start
INFO: Arrancando Coyote HTTP/1.1 en puerto http-8080
09-abr-2012 19:24:30 org.apache.jk.common.ChannelSocket init
INFO: JK: ajp13 listening on /0.0.0.0:8009
09-abr-2012 19:24:30 org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/28 config=null
09-abr-2012 19:24:30 org.apache.catalina.startup.Catalina start
INFO: Server startup in 1011 ms

INFO: Server startup in 1424 ms
```

10. Una vez verificado el arranque correcto de Tomcat, posicionarse en el subdirectorio **bin/** de la instalación de Tomcat, y detenerlo mediante el comando **./shutdown.sh**:

```
[openam@descorso01 bin]$ ./shutdown.sh

Using CATALINA_BASE: /opt/software/tomcat
Using CATALINA_HOME: /opt/software/tomcat
Using CATALINA_TMPDIR: /opt/software/tomcat/temp
```

```
Using JRE_HOME:      /opt/software/jdk1.6.X
Using CLASSPATH:     /opt/software/tomcat/bin/bootstrap.jar
```

11. Repetir los pasos anteriores (del 2 al 9) en el segundo servidor Linux donde se va a desplegar OpenAM.

4.3.2 Configuración de SSL

El proyecto requiere que las comunicaciones con el servidor de aplicaciones se realice por SSL (HTTPS), para ello se deberá configurar apropiadamente la publicación por https dentro del servidor de aplicaciones elegido. Se recomienda además no permitir el acceso al servidor por Http.

A continuación se incluye un ejemplo de configuración para servidor de aplicaciones Tomcat.

Para que OpenAM pueda trabajar en modo SSL, será necesario configurar el conector SSL en el Tomcat, y un fichero de credenciales que permita la comunicación segura con el servidor de aplicaciones. Para realizar esta configuración deben seguirse los pasos que se detallan a continuación:

1. Con el usuario **openam**, copiar el fichero PKCS12 proporcionado por la Junta de Andalucía correspondiente al entorno que se está desplegando, en el directorio **\$TOMCAT/conf** del servidor Linux.

Donde **\$TOMCAT** es el directorio de instalación de Apache-Tomcat, por ejemplo `/opt/software/tomcat`

2. Editar con VI el fichero **\$TOMCAT/conf/server.xml**, y localizar el conector del puerto **8443**

NOTA: la línea del conector comienza con `<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"`

3. Descomentar las líneas referentes al conector del puerto 8443. Al final el conector tiene que quedar como se muestra a continuación:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
     This connector uses the JSSE configuration, when using APR, the
     connector should be using the OpenSSL style configuration
     described in the APR documentation -->

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="ruta_fichero.p12"
    keystorePass="password_fichero_p12"
    keystoreType="PKCS12"
    clientAuth="false" sslProtocol="TLS" />
```

Donde se especificarán los siguientes parámetros:

- keystoreFile: Fichero de credenciales en formato PKCS12, correspondiente al entorno que se está configurando. El fichero debe estar copiado en **\$TOMCAT/conf/**
- keystorePass: Contraseña del fichero de credenciales
- keystoreType: Formato del fichero de credenciales, siempre será **PKCS12**

4. Guardar el fichero y cerrar el editor VI.
5. Arrancar el servidor Tomcat, con usuario **openam** y ejecutando el comando **\$TOMCAT/bin/startup.sh**.

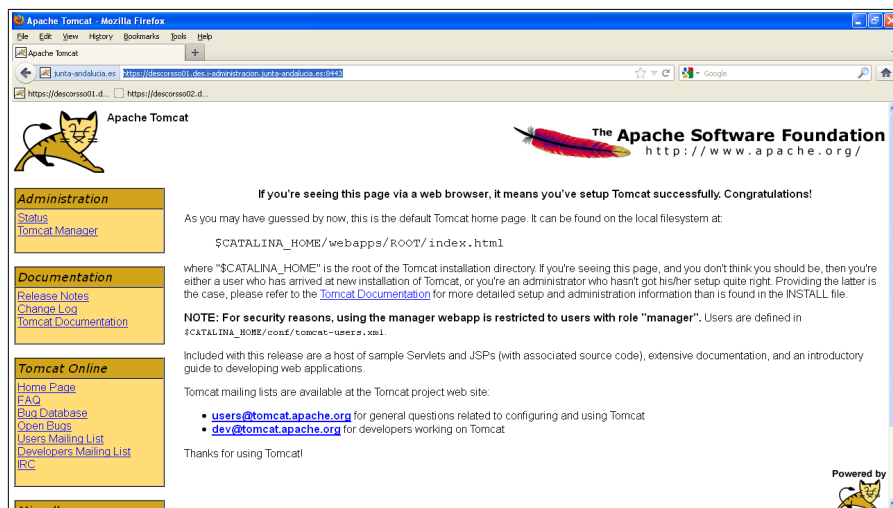
```
[openam@descorso01 bin]$ ./startup.sh

Using CATALINA_BASE: /opt/software/tomcat
Using CATALINA_HOME: /opt/software/tomcat
Using CATALINA_TMPDIR: /opt/software/tomcat/temp
Using JRE_HOME: /opt/software/jdk1.6.
Using CLASSPATH: /opt/software/tomcat/bin/bootstrap.jar
```

6. Verificar que los dos puertos definidos en Tomcat (8080 y el 8443) están escuchando peticiones:

```
[openam@descorso01 bin]$ netstat -an | grep 8080
tcp    0    0 :::8080          :::*              LISTEN
[openam@descorso01 bin]$ netstat -an | grep 8443
tcp    0    0 :::8443          :::*              LISTEN
```

7. Abrir un navegador (Internet Explorer o Firefox), y conectarse a la siguiente URL: **https://<nombre_completo_servidor>:<ssl_port>**. (donde <nombre_completo_servidor> es el nombre FQDN del servidor Linux que se está configurando) Verificar que se muestra la página de inicio de Tomcat:



8. Una vez verificado el arranque correcto de Tomcat, posicionarse con usuario **openam** en el subdirectorio **bin/** de la instalación de Tomcat, y detenerlo mediante el comando **./shutdown.sh**:

```
[openam@descorso01 bin]$ ./shutdown.sh

Using CATALINA_BASE: /opt/software/tomcat
Using CATALINA_HOME: /opt/software/tomcat
Using CATALINA_TMPDIR: /opt/software/tomcat/temp
Using JRE_HOME: /opt/software/jdk1.6.X
Using CLASSPATH: /opt/software/tomcat/bin/bootstrap.jar
```

9. Repetir todos estos pasos (del 1 al 8) en el segundo servidor Linux donde se va a desplegar OpenAM

4.3.3 Configuración de los parámetros de arranque del servidor de aplicaciones

El servidor de aplicaciones empleado debe ser parametrizado conforme al entorno donde va a ejecutarse. En concreto se recomienda optimizar el uso de memoria empleado por el servidor de aplicaciones asignando un **MaxPermSize** de 256M, y un **mínimo de 2048Mb** para entornos productivos.

A continuación se detalla como realizar esta parametrización en el arranque de Tomcat::

1. Iniciar sesión mediante SSH en el primer servidor Linux donde se está desplegando, con usuario **openam**.
2. Posicionarse en el subdirectorio **\$TOMCAT/bin/** de la instalación de

Tomcat, y detenerlo mediante el comando **./shutdown.sh**:

```
[openam@descorso01 bin]$ ./shutdown.sh  
  
Using CATALINA_BASE: /opt/software/tomcat  
Using CATALINA_HOME: /opt/software/tomcat  
Using CATALINA_TMPDIR: /opt/software/tomcat/temp  
Using JRE_HOME: /opt/software/jdk1.6.X  
Using CLASSPATH: /opt/software/tomcat/bin/bootstrap.jar
```

3. Una vez detenidos los servicios, editar con VI el fichero **startup.sh**
4. Posicionarse en el comienzo del fichero, y editar las siguientes líneas:

```
export JAVA_HOME=/opt/software/jdk1.6.X  
export JAVA_OPTS="-Xmx2048M -XX:MaxPermSize=256M"
```

5. Repetir los pasos en los restantes nodos.

4.4 Configuración del desplegable.

Sera necesario realizar una serie de pasos de configuración dentro del desplegable proporcionado por el proyecto (opensso.war).

La configuración del desplegable puede realizarse directamente sobre el fichero war descomprimiéndolo y volviéndolo a generar, o desplegando primero la aplicación en el servidor de aplicación y modificando directamente los ficheros desde el directorio webapps.

4.4.1 Compilación del módulo.

Los fuentes del módulo de autenticación están disponibles en la carpeta afirmaauth.

El desplegable dispone ya de una versión compilada de dicho módulo, si se desea sustituir dicho módulo por una versión compilada propia, realice los siguientes pasos:

1. Compilación del módulo. Sitúese en la carpeta afirmaauth y ejecute el comando.
`mvn clean package`
2. Copie el fichero afirmaauth/target/afirmaauth-1.0.jar dentro del war en el directorio opensso/WEB-INF/lib/

4.4.2 Personalización páginas del SSOWeb para cada entorno/dominio.

Las página de login y directorio de aplicaciones del SSOWeb pueden ser personalizadas en su totalidad para adaptarla a los requisitos de cada entorno/dominio y al número de aplicaciones integradas.



En cada instalación nueva de SSOWeb debe evaluarse si estas páginas han de ser modificadas o no.

1. Durante el procedimiento de instalación del SSOWeb se deberá verificar que los enlaces presentes en la página de login de cada dominio enlazan a las aplicaciones correctas para ese dominio y entorno.

En concreto se deberá revisar que los enlaces presentes bajo la sección “Gestión Cuenta” e “Información para el Usuario” son correctos para cada entorno (producción o pruebas) y dominio (guia o correo).

Para personalizar dichas página se deberá modificar los siguientes ficheros.

`opensso/config/auth/opensso/services/correo/html/Login.jsp`

`opensso/config/auth/opensso/services/guia/html/Login.jsp`

2. Durante toda la vida del proyecto, se recomienda adaptar con cada nueva aplicación integrada dentro del ssoweb, la página de directorio de aplicaciones del correspondiente dominio.



Para personalizar dichas página se deberá modificar los siguientes ficheros.

Para el dominio correo → `opensso/jda/directorio_correo.jsp`

Para el dominio guia → `opensso/jda/directorio_guia.jsp`

4.4.3 Configuración Applet @Firma y Conexión con @Firma

Dentro del proyecto se emplea dos componentes de @firma: el applet de firma y el core de @firma. El applet es empleado dentro del módulo de autenticación Afirma, como base para implementar el mecanismo de login por certificados. Los servicios del núcleo de @firma se usan para la verificación y validación del certificado de usuario. Ambos componentes de @firma tienen su propia configuración, la cual se detalla a continuación.

1. Configuración del Applet de @Firma. Dentro del directorio `opensso/afirmaApplet` se encuentra desplegado el Applet de @firma.
 - Editar el fichero “`constantes.js`” para que los campos `base` y `baseDownloadURL`, coincidan con el entorno donde se despliega la aplicación.
 - Repetir la configuración para todos los nodos.
2. Configuración del Cliente de @Firma. Dentro del directorio `opensso/WEB-INF/classes/jdaConf` se encuentran los ficheros de configuración del cliente de @firma.

Configurar los ficheros **`securityConfiguration.properties`** y **`webServicesConfiguration.properties`** con los datos de conexión de

@firma proporcionados por administración electrónica.

El directorio ya posee unos ficheros de ejemplo preconfigurados, en los que únicamente deberá configurarse la cuenta de @firma proporcionada y el servidor de @firma empleado.

Nota: Si no ha sido dado de alta previamente, el certificado SSL de @firma deberá darse de alta en el cacerts de la máquina virtual de java o en el correspondiente truststore.

```
keytool -import -file certificado_afirma.cer -trustcacerts -keystore  
[ruta_cacerts]
```

3. Repetir los pasos anteriores en cada uno de los nodos del cluster y reiniciar cada nodo.

4.5 Despliegue de la aplicación

Desplegar la aplicación modificada en el punto anterior (4.4 Configuración del desplegable.) en los correspondientes servidores de aplicaciones: nodo principal y secundarios.

Nota: Respetar el despliegue bajo el dominio /opensso.

5 Servidor primario de OpenAM

5.1 Configuración de la instancia principal de OpenAM

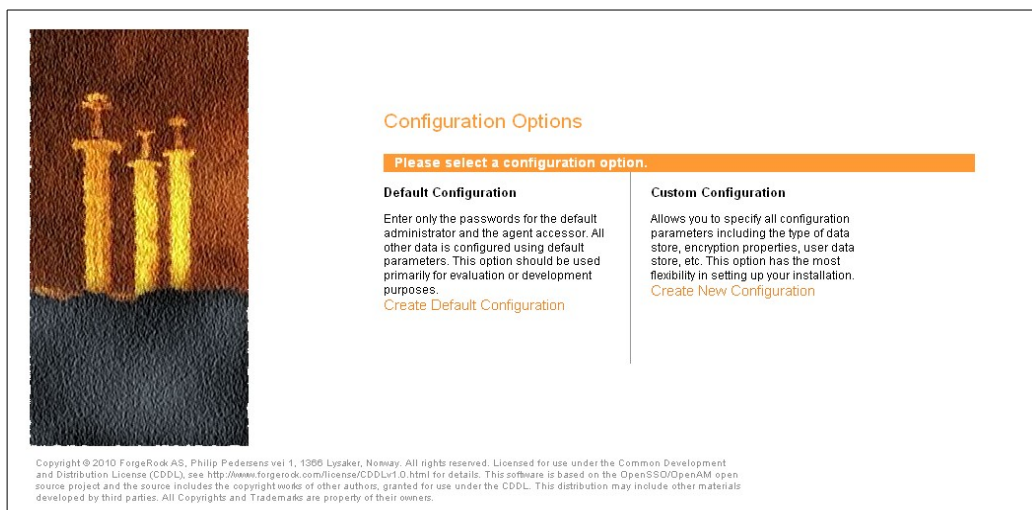
- 1) Acceder mediante un navegador web a la URL de la aplicación web desplegada:

https://<nombre_completo_servidor>[:<puerto ssl>]/opensso

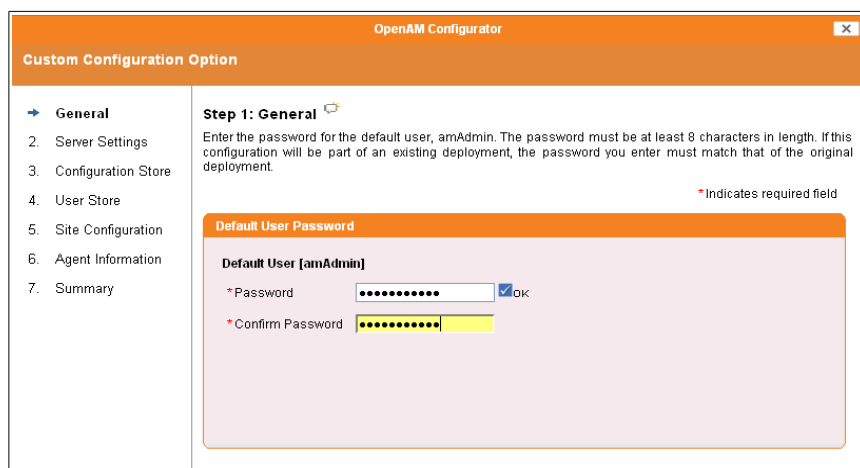
pej: <https://ssoweb.int.i-administracion.junta-andalucia.es/opensso>

Donde <nombre_completo_servidor> es el FQDN (*fully qualified domain name*) del primer servidor donde se ha desplegado OpenAM.

- 2) Se mostrará una página web de inicio de configuración del producto:



- 3) Pulsar en “**Create New Configuration...**”; se mostrará la primera página del OpenAM Configurator. Introducir la contraseña del administrador de la consola (**amadmin**). Si la contraseña cumple los requisitos de calidad (mínimo 8 caracteres, y debe incluir mayúsculas y minúsculas), se mostrará un botón de OK a la derecha de la contraseña. Una vez introducida la contraseña y la confirmación, pulsar en “**Next**” (en la parte inferior de la ventana).



4) En la siguiente ventana de configuración del servidor, especificar los parámetros de configuración de OpenAM:

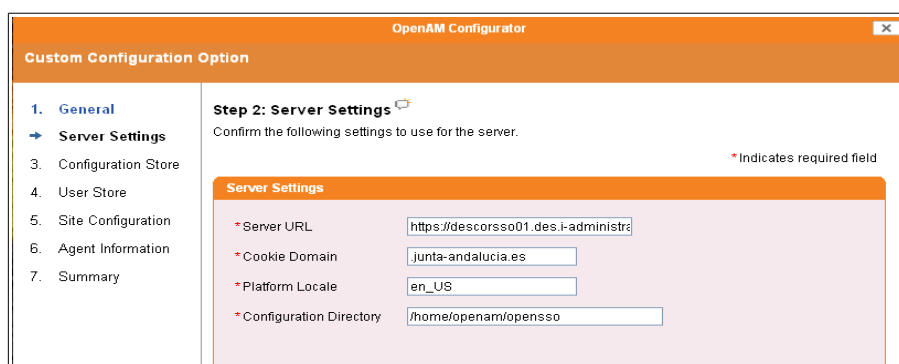
- Server URL: FQDN del servidor de OpenAM, especificando **https** y el puerto SSL. Nota: FQDN del nodo, no del cluster.

Por ejemplo: *https://descorss01.des.i-administracion.junta-andalucia.es:8443*

- Dominio de la cookie de autenticación: **.junta-andalucia.es**
- Localización de la plataforma: **es_ES**
- Directorio local de configuración de OpenAM:

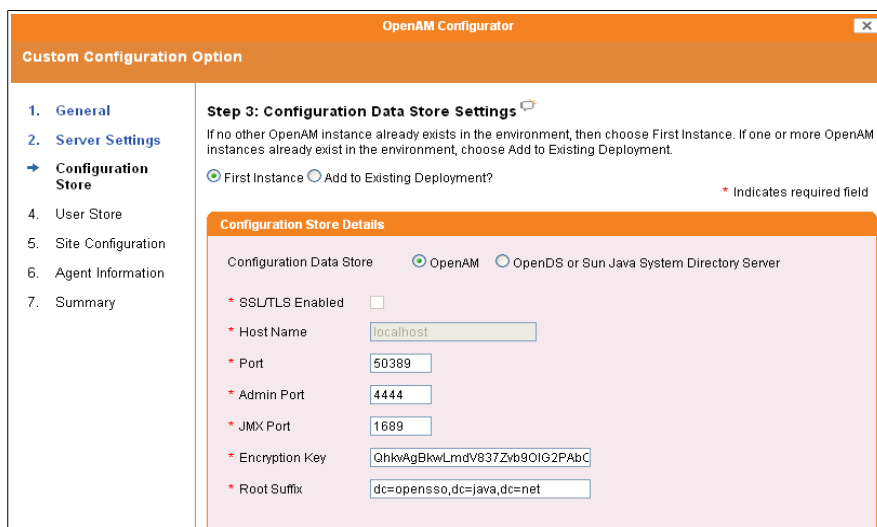
Por ejemplo **/opt/openam/opensso**

Una vez introducidos estos datos, pulsar **Next** para continuar (en la parte inferior de la ventana).



5) En la siguiente ventana, el asistente web de configuración solicitará los datos del repositorio de datos de configuración (OpenDS embebido). Dejar los datos que aparecen por defecto, y **copiar el dato contenido en "Encryption Key"**, ya que será necesario para configurar los siguientes

nodos del cluster. A continuación pulsar **Next**:



The screenshot shows the 'OpenAM Configurator' window with the 'Custom Configuration Option' tab selected. The left sidebar lists steps: 1. General, 2. Server Settings, 3. Configuration Store (highlighted), 4. User Store, 5. Site Configuration, 6. Agent Information, and 7. Summary. The main area is titled 'Step 3: Configuration Data Store Settings' and includes instructions: 'If no other OpenAM Instance already exists in the environment, then choose First Instance. If one or more OpenAM Instances already exist in the environment, choose Add to Existing Deployment.' Below this are radio buttons for 'First Instance' (selected) and 'Add to Existing Deployment?'. A section titled 'Configuration Store Details' contains the following fields: 'Configuration Data Store' with radio buttons for 'OpenAM' (selected) and 'OpenDS or Sun Java System Directory Server'; 'SSL/TLS Enabled' with an unchecked checkbox; 'Host Name' with a text box containing 'localhost'; 'Port' with a text box containing '50389'; 'Admin Port' with a text box containing '4444'; 'JMX Port' with a text box containing '1689'; 'Encryption Key' with a text box containing 'QhkwAgBkwLmdV837Zyb90IG2PAbC'; and 'Root Suffix' with a text box containing 'dc=opensso,dc=java,dc=net'. A legend indicates that an asterisk (*) denotes a required field.

- 6) En la siguiente ventana se solicitan los datos de configuración del repositorio LDAP de usuarios para el dominio raíz /. Seleccionaremos OpenAM User Data Store.

Nota: La configuración de los repositorios de identidades de GUIA y Correo se realizará más tarde mediante subdominios. El dominio raíz, sólo será usado para la consola de administración del producto y únicamente permitirá su login mediante las cuentas de administración que se den de alta dentro del repositorio de usuarios propio de OpenAm.

Opciones de configuración personalizadas

- General
- Preferencias del servidor
- Almacén de configuración
 - Almacén de usuarios
- Configuración del sitio.
- Información del agente
- Resumen

Paso 4: Configuración del almacén de usuario

Puede utilizar el almacén de datos incluido con el almacén de datos de configuración de OpenAM, o bien utilizar un almacén de datos de usuario diferente. Un procedimiento recomendado para configurar entornos de producción consiste en utilizar un almacén de datos de usuario externo diferente al almacén de datos de usuario de OpenAM. Tenga en cuenta que el servicio de directivas y el módulo de autenticación de LDAP estarán configurados para utilizar el ND del administrador de directorios y la contraseña facilitadas aquí.

☒ Almacén de datos de usuario de OpenAM
☐ Otro almacén de datos de usuario

* Indica un campo obligatorio

Detalles del almacén de usuario

❗ El uso del almacén de datos de usuario de OpenAM sólo es compatible a efectos de demostración o en entornos de desarrollo. El almacén de datos de usuario de OpenAM no es compatible en los entornos de producción.

Anterior Siguiente Cancelar

- 7) En el paso **5.Site Configuration**, marcar **No** y pulsar **Next** (las propiedades del servicio balanceado se configurarán más adelante.)

OpenAM Configurator

Custom Configuration Option

- General
- Server Settings
- Configuration Store
- User Store
 - Site Configuration
- Agent Information
- Summary

Step 5: Site Configuration

Will this instance be deployed behind a load balancer as part of a site configuration?

☒ No
☐ Yes

* Indicates required field

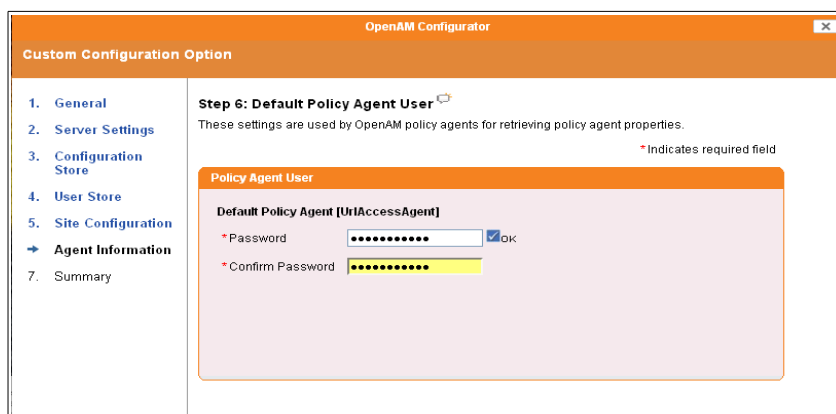
Site Configuration Details

This is the first instance of OpenAM, and no site configurations currently exist. To create a new site configuration, provide the following information

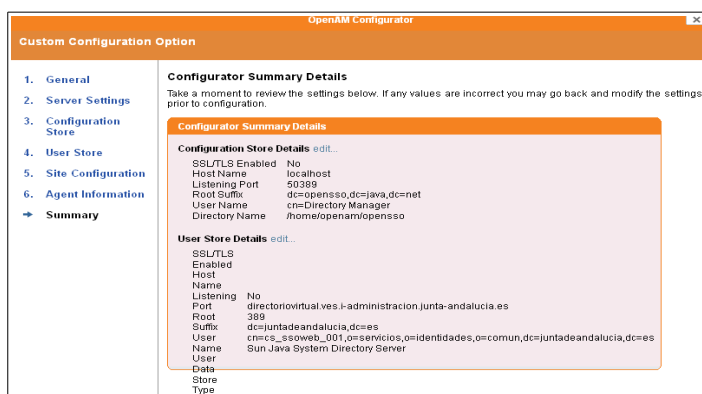
* Site Name

* Load Balancer URL

- 8) En el paso 6, introducir y confirmar la contraseña del **Policy Agent User** (no puede coincidir con la del usuario administrador **amadmin**), y pulsar **Next**.

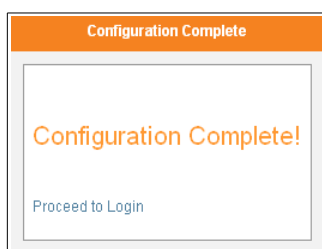


- 9) En la última ventana del asistente web, se mostrará un resumen de la configuración. Revisar la configuración, y pulsar en **“Create Configuration”** para realizar la configuración del producto:



| Configurator Summary Details | |
|--|---|
| Configuration Store Details edit... | |
| SSL/TLS Enabled | No |
| Host Name | localhost |
| Listening Port | 50399 |
| Root Suffix | dc=opensso,dc=java,dc=net |
| User Name | cn=Directory Manager |
| Directory Name | /home/openam/opensso |
| User Store Details edit... | |
| SSL/TLS Enabled | No |
| Host Name | directoriovirtual.ves.i-administracion.junta-andalucia.es |
| Listening Port | 389 |
| Root Suffix | dc=juntadeandalucia,dc=es |
| User Name | cn=cs_ssoweb_001,dc=servicios,dc=identidades,dc=comun,dc=juntadeandalucia,dc=es |
| User Store Name | Sun Java System Directory Server |
| Data Store Type | |

- 10) Tras un par de minutos, y si la configuración se completa correctamente, se mostrará un mensaje de configuración completada .



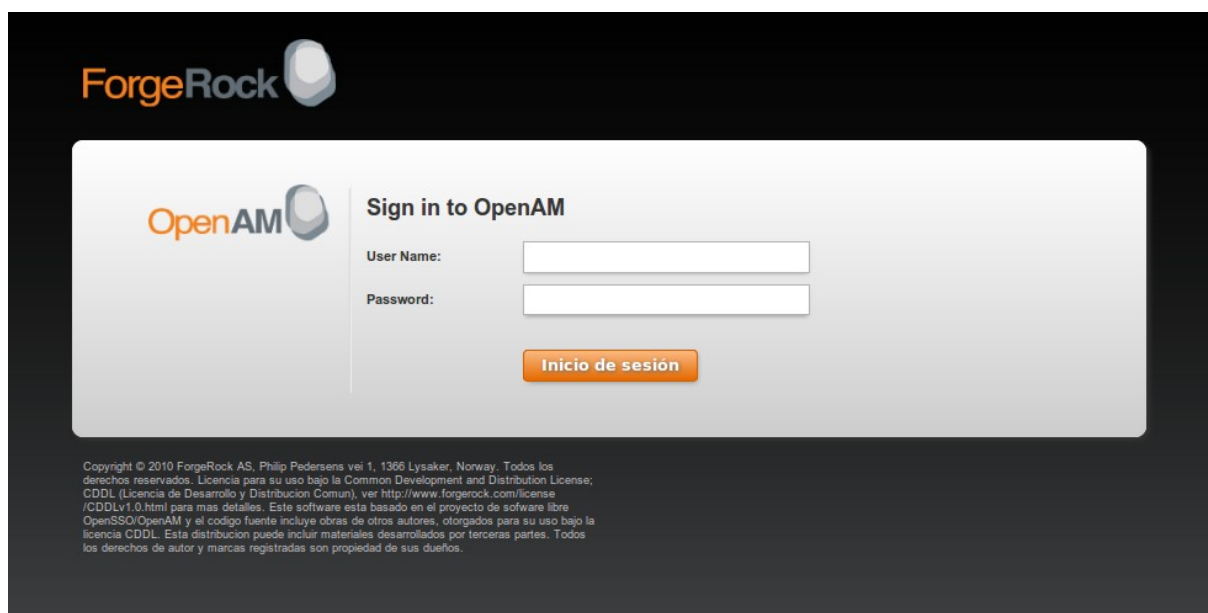
- 11) Para comprobar que la instalación de OpenAM se ha hecho correctamente acceder a la consola de administración introduciendo la url : `https://[dns_ssoweb]:[ssl puerto]/opensso/console`

pej: <https://ssoweb.int.i-administracion.junta-andalucia.es:8443/opensso/console>

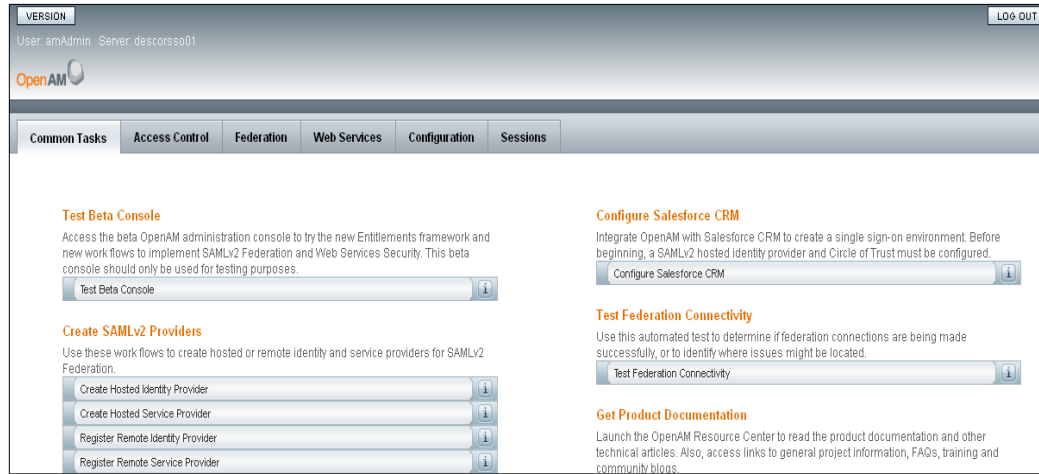
Acceder mediante el usuario amadmin y las password configurada anteriormente.

Nota: El producto se configuré con tres dominios: administración, guía y correo. El dominio de administración se accede mediante /opensso/console y ha de mostrarse la página de login original del producto.

Nota2: Este dominio de administración, no es el dominio por defecto (correo corporativo), por lo que si el producto pierde la sesión (timeout) cuando se trabaja sobre este dominio, puede llegar a mostrar las páginas de error correspondientes al dominio por defecto. Si esto sucede, no es un error de la aplicación, simplemente el producto ha eliminado la sesión pasado el correspondiente timeout y se deberá volver a iniciar sesión mediante la url `https://[dns_ssoweb]:[ssl puerto]/opensso/console`



- 12) Si la autenticación se realiza correctamente, se mostrará la consola de administración de OpenAM:



5.2 Configuración de los dominios GUIA y correo.

5.2.1 Instalación Administration Tools

Aunque los dominios pueden ser configurados a través de la consola de administración de openam, la cantidad de parámetros a configurar hace recomendable su configuración a través de la herramienta **ssoadm** en su versión de comando del sistema, empleando los backups previamente generados en el proyecto. ssoadm también tiene una versión web ssoadm.jsp. Para obtener más información acerca de la instalación de ssoadm consultar la pg: <http://docs.forgerock.org/en/openam/10.0.0/install-guide/index/chap-install-tools.html>

1. Copiar el fichero "**tools/ssoAdminTools.zip**" proporcionado por el producto, en un directorio del servidor, por ejemplo en el home del usuario **/home/openam/**
2. Cambiar los permisos de ejecución del fichero **ssoAdminTools.zip** a 750, y propietario **openam** (si este se ha copia con un usuario distinto de openam):

```
[openam@descorss01]# chown openam:openam ssoAdminTools.zip  
[openam@descorss01]# chmod 750 ssoAdminTools.zip  
-rwxr-x--- 1 openam openam 74450948 abr 10 10:19 ssoAdminTools.zip
```

3. Con el usuario **openam**, descomprimir el fichero "**ssoAdminTools.zip**" con **unzip**, directamente en el directorio de trabajo: **/home/openam/**
unzip ssoAdminTools.zip
4. Verificar que la variable JAVA_HOME está correctamente configurada

```
[openam@descorss01] $ echo $JAVA_HOME  
/path/to/jdk1.6
```

5. Ejecutar el script **./setup.sh**, obtenido tras la descompresión de ssoAdminTools.zip, en el directorio de trabajo, y configurar adecuadamente.

```
[openam@descorss01]# $ ./setup  
Ruta a los archivos de configuración del servidor OpenAM  
[/home/openam/openam]:/home/openam/opensso  
Directorio de depuración [/home/openam/tools/debug]:
```

Directorio de registro [/home/openam/tools/log]:

Las secuencias de comandos se han configurado correctamente en el directorio: /home/openam/tools/opensso

El directorio de depuración es /home/openam/tools/debug.

El directorio de registro es /home/openam/tools/log.

La versión de este archivo .zip de herramientas es: OpenAM 10.0.0 (2012-April-13 10:24)

La versión de la instancia del servidor es: OpenAM 10.0.0 (2012-April-13 10:24)

Nota: Es importante no perder la referencia a estos directorios, ya que será necesario conocer su ubicación para una gestión adecuada del entorno.

6. Crear fichero de password. Si se desea, se puede crear un fichero conteniendo el password del usuario amadmin para facilitar la ejecución de los comandos ssoadm.

```
$ cd opensso/bin/  
$ echo password_amadmin > .pass  
$ chmod 400 .pass
```

7. Verificar que openam funciona correctamente. El comando mostrara los servidores configurados tras su ejecución.

```
$ ./ssoadm list-servers -u amadmin -f .pass  
https://ssoweb.int.i-administracion.junta-andalucia.es:8443/opensso
```

Nota: La conexión con Openam debe realizarse sobre SSL, si el certificado SSL del servidor no ha sido registrado en el cacerts de la máquina la conexión dará errores SSL o del tipo:

```
Logging configuration class "com.sun.identity.log.s1is.LogConfigReader"  
failed  
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:  
FATAL ERROR: Cannot obtain Application SSO token.  
Check AMConfig.properties for the following properties  
    com.sun.identity.agents.app.username  
    com.ipplanet.am.service.password
```

En estos casos se deberá registrar el certificado SSL en el cacerts o añadir al fichero **ssoadm** opciones para la carga de un truststore conteniendo al mismo mediante las system properties: `javax.net.ssl.trustStore` y `javax.net.ssl.trustStorePassword`



Servicio de WebSSO
Manual de instalación y configuración

**Consejería de Economía,
Innovación y Ciencia**

```
-D"javax.net.ssl.trustStore=/path/to/keystore.jks"  
-D"javax.net.ssl.trustStorePassword=password_keystore"
```

5.2.2 Registro del módulo de autenticación Afirma en Openam

El proyecto ha desarrollado un módulo de autenticación para el login con usuario/password y certificados.

Este debe registrarse dentro de openam para que pueda ser empleado desde los dominios correo y guía.

El registro tiene dos pasos: el alta del servicio y el registro del módulo. Estas operaciones pueden realizarse a través de la utilidad ssoadm, ya sea en su versión de consola o web (ssoadm.jsp).

1. Registro del Servicio.

```
./ssoadm create-svc --adminid amadmin --password-file .pass --xmlfile  
[ruta_tomcat_webapp]/opensso/WEB-INF/classes/amAuthAfirma.xml  
Service was added.
```

2. Registro del módulo de autenticación.

```
./ssoadm register-auth-module --adminid amadmin --password-file .pass  
--authmodule es.juntadeandalucia.openam.afirmaauth.Afirma  
Authentication module was registered.
```


5.2.3 Configuración dominio correo

5.2.3.1 Crear el dominio.

El dominio de correo puede crearse directamente desde la consola de administración web accediendo a la pestaña de Control de acceso, o empleando la utilidad ssoadm.

El nombre del dominio debe ser “correo” y no otro, ya que el desplegable del proyecto ha sido configurado previamente con este nombre de dominio. Si se desea cambiar este nombre de dominio, se deberá adaptar el proyecto (carpetas de plantillas y dominio por defecto) conforme al nuevo nombre de dominio.



Mediante ssoadm el dominio se crearía con el siguiente comando:

```
./ssoadm create-realm --realm correo -u amAdmin -f .pass
```

5.2.3.2 Crear y configurar el DataStore.

Debido a la cantidad de parámetros de configuración existente, se recomienda realizar la creación del datastore (Almacén de datos) a través del comando ssoadm y el backup proporcionado por el proyecto.

1. Crear el datastore.

```
./ssoadm create-datastore -e correo -m correo -t LDAPv3 -u amAdmin -f .pass -D correo_datastore.txt
```

2. Configuración del datastore. Se deberá configurar el datastore creado en el paso anterior para su conexión a los directorios LDAPs correspondientes.

Dentro de Control de Acceso → Dominio correo -> Almacén de datos, acceder al datastore correspondiente haciendo click sobre su nombre.

VERSION: CERRAR SESIÓN

Usuario: amAdmin Servidor: prucorsa01

OpenAM

null Guardar Restablecer Volver a Almacenes de datos

* Nombre: correo_pruebas * Indica que el campo es obligatorio

Cargar esquema tras guardar: ☐

Server Settings

* Servidor LDAP

Valores actuales: 10.240.234.17:389 10.240.234.70:389 Eliminar

Nuevo valor: Agregar

Formato: nombre de host del servidor LDAP:puerto | ID_servidor | ID_silo

DN de enlace de LDAP: cn=admin,c=es Un usuario o administrador que dispone de los suficientes derechos de acceso para realizar las operaciones admitidas.

Contraseña de enlace de LDAP:

Configurar adecuadamente los valores de conexión al ldap de correo:

1. Servidores ldap. Configurar los servidores LDAP correspondientes. Nota: openam accederá siempre al primer ldap configurado, si este falla, se probará con los siguientes ldaps configurados.
2. DN de enlace de ldap: Cuenta ldap para el acceso a los ldaps configurados en el paso anterior. Se requiere un usuario sin restricciones: de búsqueda, profundidad, lectura de campos, etc.
No se recomienda emplear cuentas con permiso de escritura sobre el directorio, para evitar que una mala configuración del producto pueda crear entradas en el mismo.
3. Contraseña ldap del usuario configurado en el campo anterior. La utilidad de configuración no carga la clave, es el comportamiento normal, hay que ponerla a mano
3. Una vez creado el datastore, deberá eliminarse los datastores por defecto que hayan sido creados durante el alta del dominio, de forma que únicamente esté disponible el que hemos creado en el paso anterior, para ello:

Acceder a la consola de administración de openam y logarse como administrador.

Pej: <http://ssoweb.int.i-administracion.junta-andalucia.es:8080/opensso/console>

Acceder a

Control de Acceso → Dominio correo-> Almacén de datos.

Eliminar todos los datastores (embedded) excepto el creado en el paso anterior.

VERSION CERRAR SESIÓN

Usuario: amAdmin Servidor: usuario-laptop7

OpenAM

General Autenticación Servicios Almacenes de datos Privilegios Directivas Asuntos Agentes

/ (dominio de nivel superior) > correo

correo - Almacenes de datos Volver a Control de acceso

Almacenes de datos (2 Elemento(s))

Nuevo... Borrar

| <input checked="" type="checkbox"/> <input type="checkbox"/> | Nombre | Tipo |
|--|----------|--------|
| <input type="checkbox"/> | correo | LDAPv3 |
| <input type="checkbox"/> | embedded | OpenDJ |

4. Verificar el correcto funcionamiento del datastore.

Para verificar el correcto funcionamiento del datastore, acceder a Control de Acceso → Dominio correo-> Asuntos.

Deberá aparece un listado de usuarios contenidos en el directorio de correo.

VERSION CERRAR SESIÓN

Usuario: amAdmin Servidor: usuario-laptop7

OpenAM

General Autenticación Servicios Almacenes de datos Privilegios Directivas Asuntos Agentes

Usuario

/ (dominio de nivel superior) > correo

Usuario Volver a Control de acceso

*

Usuario (1 - 25 de 100)

Nuevo... Borrar

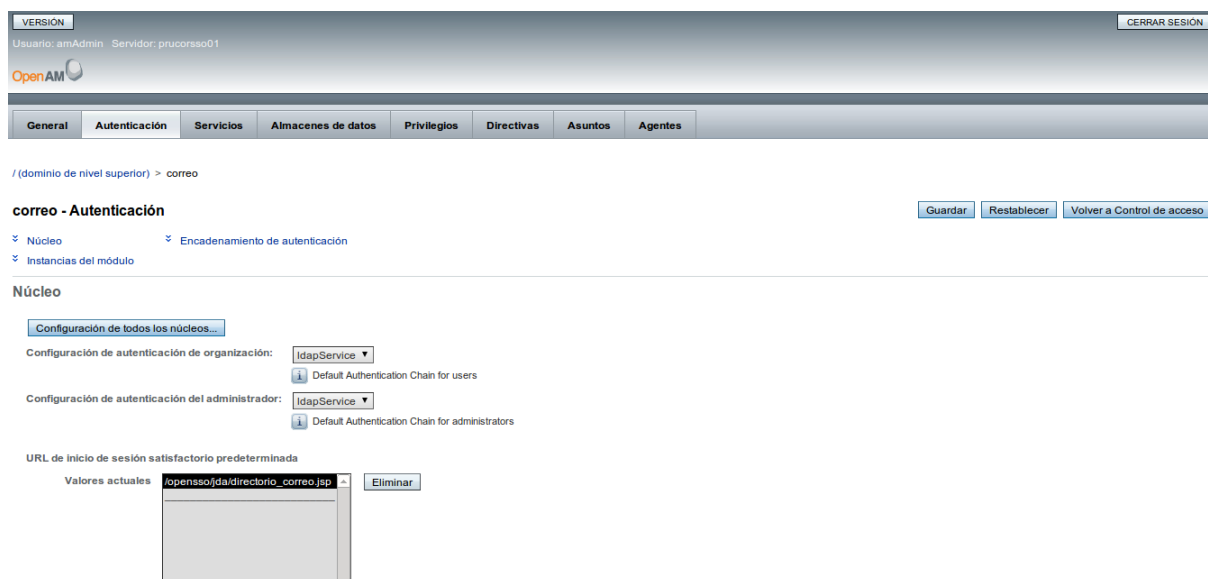
| <input checked="" type="checkbox"/> <input type="checkbox"/> | Nombre | Id. universal |
|--|----------|--------------------------|
| <input type="checkbox"/> | 15373019 | manuviso.averroes |
| <input type="checkbox"/> | 24131377 | frarova.averroes |
| <input type="checkbox"/> | 24168594 | quijote.averroes |
| <input type="checkbox"/> | 27230151 | mparra.averroes |
| <input type="checkbox"/> | 27317123 | sasuva.averroes |
| <input type="checkbox"/> | 27325843 | vicentepimentel.averroes |
| <input type="checkbox"/> | 28590415 | doloresanchez.averroes |
| <input type="checkbox"/> | 28686263 | catan.averroes |

5.2.3.3 Configuración del procedimiento de Autenticación.

En este apartado se configura el módulo de autenticación de usuarios para el dominio correspondiente.

En este apartado se configurará como único módulo de autenticación disponible para el dominio, el desarrollado bajo el proyecto (Afirma), y se configurará para que permita al usuario la autenticación mediante: usuario/password (con uid y nif) y certificado digital (FNMT).

1. Acceder a Control de Acceso → Dominio **Correo**-> Autenticación



2. Cambiar el valor del campo “**URL de inicio de sesión satisfactorio predeterminada**” a **/opensso/jda/directorio_correo.jsp**, eliminado el valor presente y creando una nueva entrada.

Nota: La página “directorio_correo.jsp” es la que se muestra cuando un usuario se loga satisfactoriamente en el sistema, haciendo login directamente desde la página de login del dominio sin haber sido redirigido previamente a través de una aplicación tercera. Cuando se accede desde una tercera aplicación esta página no se muestra ya que el usuario es redirigido a la aplicación integrada tras el logado.

Nota2: La página “directorio_correo.jsp” muestra un listado de aplicaciones integradas con el dominio de correo del SSOWeb. Si se desea personalizar esta página se deberá modificar directamente el fichero “directorio_correo.jsp”

3. Configurar el módulo de Afirma conforme a la estructura del datastore empleado.

Acceder a Control de Acceso → Dominio **Correo** → Autenticación

Instancias del módulo

| Instancias del módulo (6 elementos) | |
|--|------------------|
| <input type="button" value="Nuevo"/> <input type="button" value="Eliminar"/> | |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Nombre | Tipo |
| <input type="checkbox"/> DataStore | Almacén de datos |
| <input type="checkbox"/> Federation | Federation |
| <input type="checkbox"/> HOTP | HOTP |
| <input type="checkbox"/> LDAP | LDAP |
| <input type="checkbox"/> SAE | SAE |
| <input type="checkbox"/> WSSAuthModule | WSSAuthModule |

En “instancias de módulo” pulsar “nuevo” y crear una nueva instancia del Módulo @firma con nombre Afirma.

Nueva instancia del módulo

* Indica que el campo es obligatorio

* Nombre:

* Tipo:

- ☐ Active Directory
- ☐ Adaptive Risk
- ☐ Almacén de datos
- ☐ Anónimo
- ☐ Certificado
- ☐ Condición de miembro
- ☐ Federación
- ☐ HOTP
- ☐ HTTP Basic
- ☐ JDBC
- ☐ LDAP
- ☒ Módulo @Firma
- ☐ MSISDN
- ☐ OAuth 2.0
- ☐ RADIUS
- ☐ SAE
- ☐ SecurID
- ☐ Windows Desktop SSO
- ☐ Windows NT
- ☐ WSSAuth

Una vez creada la instancia del módulo se procederá a su configuración, para ello, en el apartado de “instancias de módulo” hacer click sobre el módulo Afirma para editar sus propiedades.



Servicio de WebSSO Manual de instalación y configuración

Consejería de Economía,
Innovación y Ciencia

VERSION CERRAR SESIÓN

Usuario: amAdmin Servidor: prucorso01

OpenAM

Módulo @Firma Guardar Restablecer Volver a Autenticación

Atributos de dominio

Authentication Level:

Campo NIF dentro del Datastore:

Campo RDN del Datastore:

Campo permitidos para hacer login

Valores actuales Eliminar

Nuevo valor Agregar

Campos NIFs devueltos por @Firma

Valores actuales Eliminar

Se deberá configurar los siguiente valores en los campos, eliminando los valores predefinidos si fuera necesario:

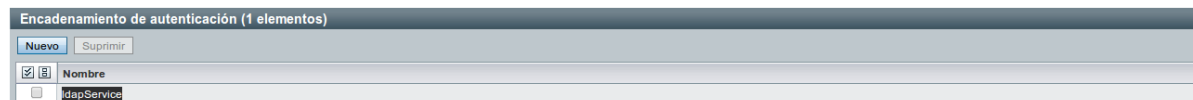
- Campo NIF dentro del Datastore: **JAdni**
Nota: Este campo identifica dentro del directorio de correo, qué campo tiene almacenado el campo nif.
- Campo RDN del Datastore: **uid**
- Campo permitidos para hacer login: dar de alta dos entradas: **uid y JAdni**
Nota: en este campo se dan de alta los entradas del directorio de correo que se emplearan para buscar el usuario introducido por el usuario en el campo de login. La configuración actual permite el login mediante cuenta de usuario (uid) y nif (JAdni), pero puede añadirse o eliminarse nuevos campos según se solicite.
- Campos Nifs devueltos por @firma: dar de alta dos entradas: **NIFResponsable y NIF-CIF**.
Nota: Este campo identifica posibles atributos devueltos por @firma que contendrán el NIF del usuario.
Nota2: Esta configuración sólo permite autenticación con **certificados de usuario** de la **FNMT** (NIFResponsable y NIF-CIF son atributos presente en certificados de usuario FNMT). Si se desea permitir otros tipos de certificado o de otras Cas, se deberán añadir en este campo el nombre de los atributos devueltos por @firma para esas CAs que contendrán el nif del usuario.
- Nif Bloqueados para login: Contiene un listado de Nif a los cuales NO se les permitirá el logado en el SSO.
Nota: El directorio de correo corporativo está lleno de cuentas que no son de usuarios o que contienen NIF ficticios. Este campo sirve para evitar el login en el sistema con una cuenta de sistema, un nif ficticio, o un usuario al que NO se desee permitir el login mediante SSO, siempre y cuando estos se hayan dado previamente de alta.

4. Configurar la cadena de autenticación.

Acceder a Control de Acceso → Dominio **Correo**-> Autenticación

Editar a la configuración de la cadena de autenticación por defecto (IdapService) haciendo click sobre su nombre.

Encadenamiento de autenticación



Cambiar la configuración para que el único módulo de autenticación sea el de Afirma y de uso obligatorio. Este apartado deberá quedar configurado como se muestra en la siguiente imagen:

IdapService - Propiedades

[Guardar](#) [Restablecer](#) [Volver a Autenticación](#)



5. Eliminar otras instancias de módulos.

Acceder a Control de Acceso → Dominio **Correo** → Autenticación

Eliminar todos los módulos de autenticación presentes en el apartado "Instancias del módulo", excepto el módulo de afirma, para evitar así posibles fallas de seguridad.

Instancias del módulo



5.2.4 Configuración dominio GUIA

5.2.4.1 Crear el dominio.

El dominio de GUIA puede crearse directamente desde la consola de administración web accediendo a la pestaña de Control de acceso, o empleando la utilidad ssoadm.

El nombre del dominio debe ser “guia” y no otro, ya que el desplegable del proyecto ha sido configurado previamente con este nombre de dominio. Si se desea cambiar este nombre de dominio, se deberá adaptar el proyecto (carpetas de plantillas y dominio por defecto) conforme al nuevo nombre de dominio.



Mediante ssoadm el dominio se crearía de la siguiente forma:

```
./ssoadm create-realm --realm guia -u amAdmin -f .pass
```

5.2.4.2 Crear y configurar el DataStore.

Debido a la cantidad de parámetros de configuración existente, se recomienda realizar la creación del datastore a través del comando ssoadm y el backup proporcionado por el proyecto.

5. Crear el datastore.

```
./ssoadm create-datastore -e guia -m guia -t LDAPv3 -u amAdmin -f .pass  
-D guia_datastore.txt
```

6. Configuración del datastore. Se deberá configurar el datastore creado en los pasos anteriores para su conexión a los directorios LDAPs correspondiente.

Dentro de Control de Acceso → Dominio **Guia** → Almacén de datos,

acceder al datastore correspondiente haciendo click sobre su nombre.

Configurar adecuadamente los valores de conexión al ldap de GUIA:

1. Servidores ldap. Configurar los servidores LDAP correspondientes. Nota: openam accederá siempre al primer ldap configurado, si este falla, se probará con los siguientes ldaps configurados.
2. DN de enlace de ldap: Cuenta ldap para el acceso a los ldaps configurados en el paso anterior. Se requiere un usuario sin restricciones: de búsqueda, profundidad, lectura de campos, etc.
No se recomienda emplear cuentas con permiso de escritura sobre el directorio, para evitar que una mala configuración del producto pueda crear entradas en el mismo..
3. Contraseña ldap del usuario configurado en el campo anterior.
7. Una vez creado el datastore, deberá eliminarse los datastores por defecto que hayan sido creados durante el alta del dominio, de forma que únicamente esté disponible el que hemos creado en el paso anterior, para ello:

Acceder a la consola de administración de openam y logarse como administrador.

Pej: <http://ssoweb.int.i-administracion.junta-andalucia.es:8080/opensso/console>

Acceder a

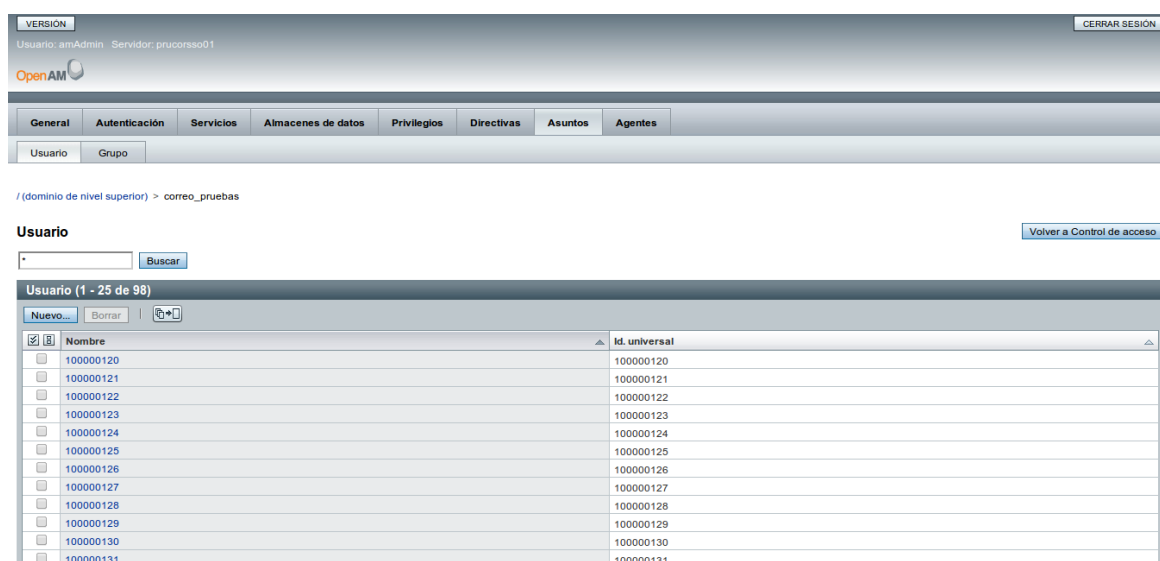
Control de Acceso → Dominio **Guia** → Almacén de datos.

Eliminar todos los datastores excepto el creado en el paso anterior.

8. Verificar el correcto funcionamiento del datastore.

Para verificar el correcto funcionamiento del datastore acceder a Control de Acceso → Dominio guía-> Asuntos.

Deberá aparecer un listado de usuarios contenidos en el directorio de guía.



VERSION CERRAR SESION

Usuario: amAdmin Servidor: prucorss01

OpenAM

General Autenticación Servicios Almacenes de datos Privilegios Directivas Asuntos Agentes

Usuario Grupo

/ (dominio de nivel superior) > correo_pruebas

Usuario Volver a Control de acceso

Nuevo... Borrar

| Nombre | Id. universal |
|-----------|---------------|
| 100000120 | 100000120 |
| 100000121 | 100000121 |
| 100000122 | 100000122 |
| 100000123 | 100000123 |
| 100000124 | 100000124 |
| 100000125 | 100000125 |
| 100000126 | 100000126 |
| 100000127 | 100000127 |
| 100000128 | 100000128 |
| 100000129 | 100000129 |
| 100000130 | 100000130 |
| 100000131 | 100000131 |

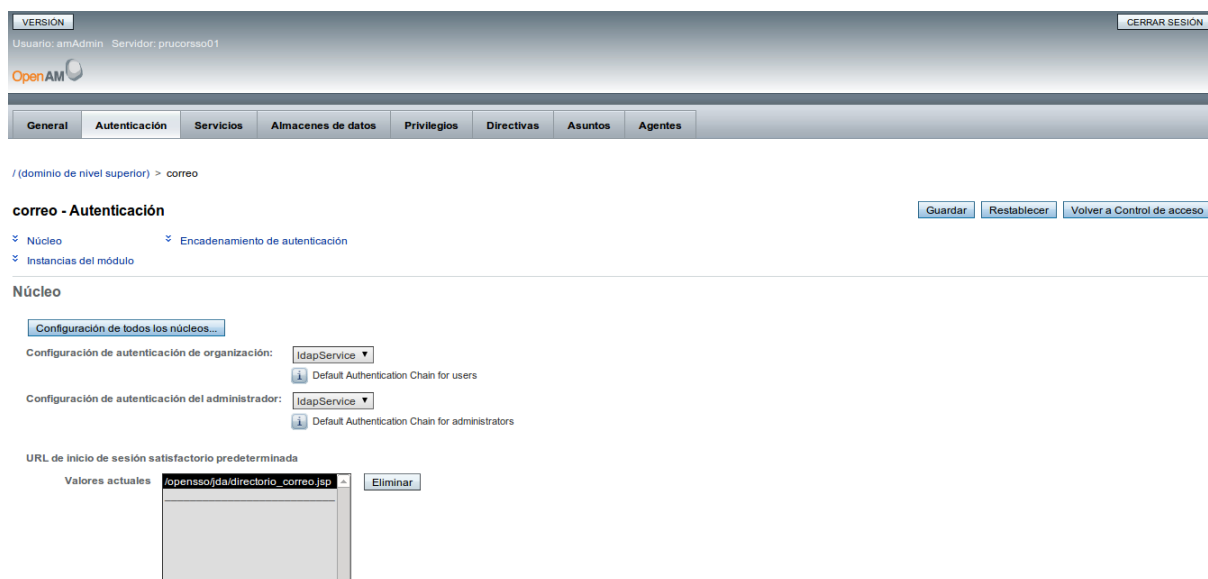
Nota: el directorio GUIA establece una conexión SSL, puede ser necesario registrar previamente en el cacerts o truststore correspondiente el certificado SSL del Idap guia.

5.2.4.3 Configuración del procedimiento de Autenticación.

En este apartado se configura el módulo de autenticación de usuarios para el dominio.

Se establece como único módulo de autenticación disponible para el dominio, el desarrollado bajo el proyecto (Afirma) y se configurará para que permita al usuario la autenticación mediante: usuario/password (con uid, nif y opcionalmente código júpiter) y certificado digital (FNMT).

1. Acceder a Control de Acceso → Dominio **GUIA** → Autenticación



The screenshot shows the OpenAM administration console. At the top, there's a header with 'VERSION' and 'CERRAR SESIÓN'. Below it, a navigation bar includes 'General', 'Autenticación', 'Servicios', 'Almacenes de datos', 'Privilegios', 'Directivas', 'Asuntos', and 'Agentes'. The main content area is titled 'correo - Autenticación' and includes buttons for 'Guardar', 'Restablecer', and 'Volver a Control de acceso'. Under the 'Núcleo' section, there are dropdown menus for 'Configuración de autenticación de organización' and 'Configuración de autenticación del administrador', both set to 'IdapService'. Below this, there's a section for 'URL de inicio de sesión satisfactorio predeterminada' with a text input field containing '/openso/jda/directorio_correo.jsp' and an 'Eliminar' button.

2. Cambiar el valor del campo “**URL de inicio de sesión satisfactorio predeterminada**” a **/openso/jda/directorio_guia.jsp**, eliminando la entra existente y añadiendo la nueva. **A continuación salvar los cambios.**

Nota: La página “directorio_guia.jsp” es la que se muestra cuando un usuario se loga satisfactoriamente en el sistema haciendo login directamente desde la página del dominio sin haber sido redirigido previamente a través de una aplicación tercera.

Nota2: La página “directorio_guia.jsp” muestra un listado de aplicaciones integradas con el dominio de guia del SSOWeb. Si se desea personalizar esta página se deberá modificar directamente el fichero “directorio_guia.jsp”

3. Configurar el módulo de Afirma conforme a la estructura del datastore

empleado.

Acceder a Control de Acceso → Dominio **GUIA**-> Autenticación

Instancias del módulo

| Instancias del módulo (6 elementos) | | |
|--|---------------|------------------|
| <input type="button" value="Nuevo"/> <input type="button" value="Eliminar"/> | | |
| <input checked="" type="checkbox"/> <input type="checkbox"/> | Nombre | Tipo |
| <input type="checkbox"/> | DataStore | Almacén de datos |
| <input type="checkbox"/> | Federation | Federation |
| <input type="checkbox"/> | HOTP | HOTP |
| <input type="checkbox"/> | LDAP | LDAP |
| <input type="checkbox"/> | SAE | SAE |
| <input type="checkbox"/> | WSSAuthModule | WSSAuthModule |

En “instancias de módulo” pulsar “nuevo” y crear una nueva instancia del Módulo @firma con nombre Afirma.

Nueva instancia del módulo

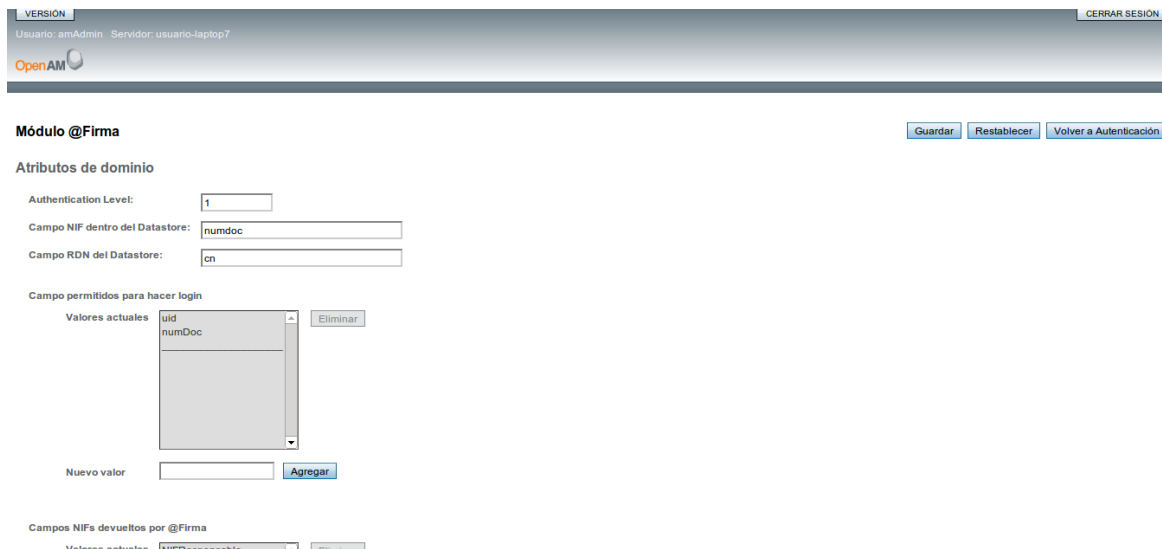
* Indica que el campo es obligatorio

* Nombre:

* Tipo:

- ☐ Active Directory
- ☐ Adaptive Risk
- ☐ Almacén de datos
- ☐ Anónimo
- ☐ Certificado
- ☐ Condición de miembro
- ☐ Federación
- ☐ HOTP
- ☐ HTTP Basic
- ☐ JDBC
- ☐ LDAP
- ☒ Módulo @Firma
- ☐ MSISDN
- ☐ OAuth 2.0
- ☐ RADIUS
- ☐ SAE
- ☐ SecurID
- ☐ Windows Desktop SSO
- ☐ Windows NT
- ☐ WSSAuth

Una vez creada la instancia del módulo se procederá a su configuración, para ellos en el apartado de “instancias de módulo” hacer click sobre el módulo Afirma para editar sus propiedades.



The screenshot shows the OpenAM configuration interface for the @Firma module. At the top, there is a header bar with the OpenAM logo and a 'CERRAR SESIÓN' button. Below the header, the 'Módulo @Firma' is selected. The 'Atributos de dominio' section contains three input fields: 'Authentication Level' (set to 1), 'Campo NIF dentro del Datastore' (set to numdoc), and 'Campo RDN del Datastore' (set to cn). The 'Campo permitidos para hacer login' section shows a list of 'Valores actuales' (uid, numDoc) with an 'Eliminar' button. Below this is a 'Nuevo valor' input field and an 'Agregar' button. The 'Campos NIFs devueltos por @Firma' section shows a list of 'Valores actuales' (NIFResponsable, NIF-CIF) with an 'Eliminar' button.

Se deberá configurar los siguiente valores en los campos, eliminando los valores predefinidos si fuera necesario:

- Campo NIF dentro del Datastore: **numdoc**
Nota: Este campo identifica dentro del directorio de guía, qué campo tiene almacenado el campo nif.
- Campo RDN del Datastore: **cn**
- Campos permitidos para hacer login: dar de alta dos entradas: **uid y numDoc**, opcionalmente si se solicita se podrá dar de alta la cuenta júpiter (codJupiter).

Nota: en este campo se dan de alta los entradas del directorio de correo que se emplearan para buscar el usuario introducido por el usuario en el campo de login. La configuración actual permite el login por cuenta (uid) y nif (numDoc), pero puede añadirse o eliminarse nuevos campos según se solicite.

- Campos Nifs devueltos por @firma: dar de alta dos entradas: **NIFResponsable y NIF-CIF**.

Nota: Este campo identifica posibles atributos devueltos por @firma que contendrán el NIF del usuario.

Nota2: Esta configuración sólo permite autenticación con **certificados de usuario** de la **FNMT** (NIFResponsable y NIF-CIF son atributos presente en certificados de usuario FNMT). Si se desea permitir otros tipos de certificado o de otras Cas, se deberán añadir en este campo el nombre de los atributos devueltos por @firma para esas CAs que contendrán el nif del usuario.

- Nif Bloqueados para login: Contiene un listado de Nif a los cuales no se les permitirá el logado en el SSO.

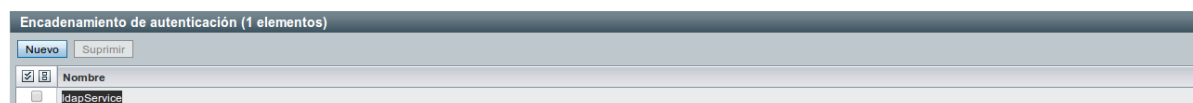
Nota: El directorio de correo corporativo está lleno de cuentas que no son de usuarios o que contienen NIF ficticios. Este campo sirve para evitar el login en el sistema con una cuenta de sistema, un nif ficticio, o un usuario al que se desee no permitir el login mediante SSO, siempre y cuando estos se hayan dado previamente de alta.

4. Configurar la cadena de autenticación.

Acceder a Control de Acceso → Dominio GUIA-> Autenticación

Editar a la configuración de la cadena de autenticación por defecto (IdapService) haciendo click sobre su nombre.

Encadenamiento de autenticación



Encadenamiento de autenticación (1 elementos)

Nuevo Suprimir

| Nombre |
|-------------|
| IdapService |

Cambiar la configuración para que el único módulo de autenticación sea el de Afirma y de uso obligatorio. Este apartado deberá quedar configurado como se muestra en la siguiente imagen:

IdapService - Propiedades

Guardar Restablecer Volver a Autenticación



(1 Elemento(s))

Agregar Eliminar Reordenar

| Instancia | Criterios | Opciones |
|-----------|-------------|----------|
| afirma | OBLIGATORIO | |

5. Eliminar otras instancias de módulos.

Acceder a Control de Acceso → Dominio GUIA-> Autenticación

Eliminar todos los módulos de autenticación presentes en el apartado "Instancias del módulo", excepto el módulo de afirma, para evitar así posibles fallas de seguridad.

5.2.5 Verificación de la instalación.

La siguiente prueba de verificación deberá realizarse dos veces, una vez por cada uno de los dominios configurados: correo y guia.

Para realizar la prueba sobre el dominio de Correo se deberán realizar los pasos indicados en este apartado accediendo a la url `https://[url_ssoweb][:ssl_port]/opensso/UI/Login?realm=correo` y empleando un usuario presente en ese dominio.

Para realizar la prueba sobre el dominio de GUIA se deberá realizar los pasos indicados a continuación accediendo a la url `https://[url_ssoweb][:ssl_port]/opensso/UI/Login?realm=guia` y empleando un usuario presente en ese

dominio.

Nota: Se recomienda cerrar el navegador cuando se desea cambiar el dominio sobre el que realizar las pruebas.

Pasos para la verificación:

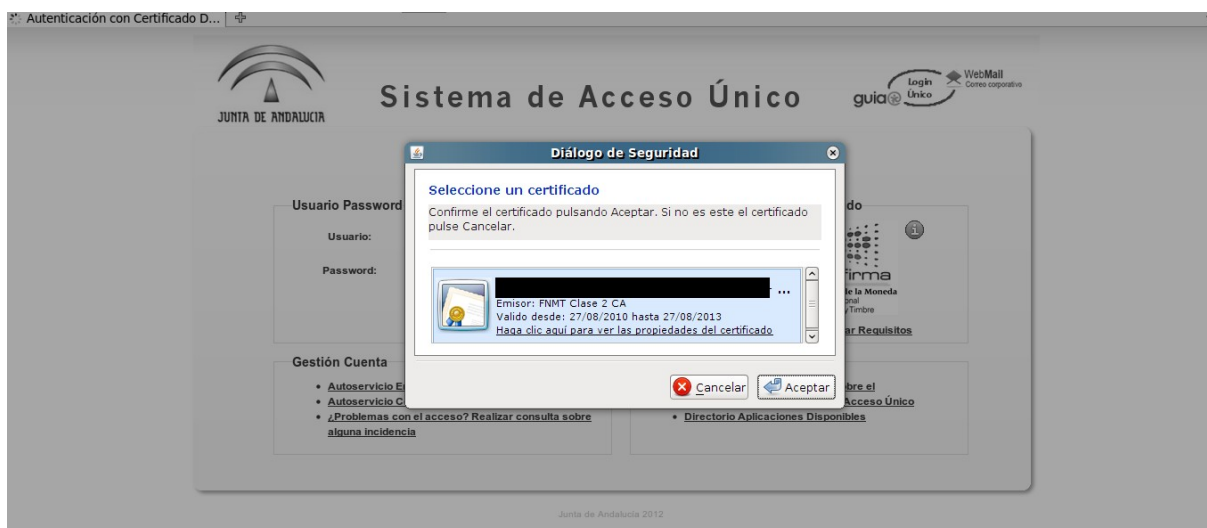
1. Con una sesión de navegador nueva acceda a la url de acceso para el dominio correspondiente.



2. Realice dos pruebas de autenticación, primero mediante uid y password y posteriormente mediante su nif y password Nota: hacer logout (enlace "salir" de la página de directorio) antes de iniciar una nueva prueba de logado. Verifique que tras cada logado se visualiza correctamente el listado de aplicaciones integradas para ese dominio.



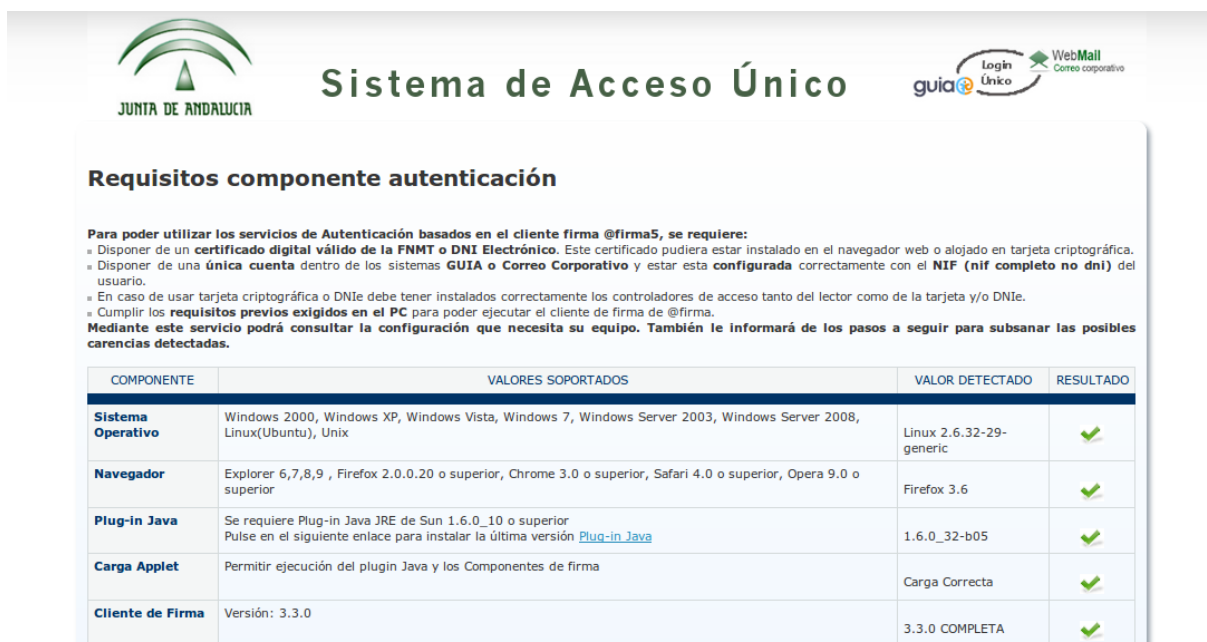
4. Realice nuevamente logout e inicie el login por certificado digital. Verifique que se visualiza el listado de aplicaciones integradas para ese dominio.



Si hubiese un error en la carga del applet de @firma, puede emplear el enlace **“¿problemas? Verificar requisitos”**.



Mediante ese enlace accederá a la utilidad de verificación de requisitos del applet de @firma.



| COMPONENTE | VALORES SOPORTADOS | VALOR DETECTADO | RESULTADO |
|--------------------------|--|-------------------------|-----------|
| Sistema Operativo | Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Linux(Ubuntu), Unix | Linux 2.6.32-29-generic | ✓ |
| Navegador | Explorer 6,7,8,9 , Firefox 2.0.0.20 o superior, Chrome 3.0 o superior, Safari 4.0 o superior, Opera 9.0 o superior | Firefox 3.6 | ✓ |
| Plug-in Java | Se requiere Plug-in Java JRE de Sun 1.6.0_10 o superior Pulse en el siguiente enlace para instalar la última versión Plug-in Java | 1.6.0_32-b05 | ✓ |
| Carga Applet | Permitir ejecución del plugin Java y los Componentes de firma | Carga Correcta | ✓ |
| Cliente de Firma | Versión: 3.3.0 | 3.3.0 COMPLETA | ✓ |

5.3 Creación de los IDPs.

5.3.1 Configuración del certificado para el IDP.

Si se desea cambiar el certificado autogenerado por openam para la firma de mensajes en el IDP, se deberá seguir los siguientes pasos:

1. Generar una nueva clave de firma y un keystore en el que almacenarla utilizando la herramienta keytool:

```
$ cd /tmp

$ keytool -genkeypair -alias newkey -keyalg RSA -keysize 1024 -validity 730
-storetype JKS -keystore keystore.jks

Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: A-rellenar
What is the name of your organizational unit?
[Unknown]: A-rellenar
What is the name of your organization?
[Unknown]: A-rellenar
What is the name of your City or Locality?
[Unknown]: A-rellenar
What is the name of your State or Province?
[Unknown]: A-rellenar
What is the two-letter country code for this unit?
[Unknown]: A-rellenar
Is CN=A-rellenar, OU=A-rellenar, O=A-rellenar, L=A-rellenar, ST=A-
rellenar, C=A-rellenar correct?
[no]: yes

Enter key password for <newkey>
(RETURN if same as keystore password):

Re-enter new password:
```

2. Los ficheros .keypass y .storepass, presentes en el directorio de configuración, deben contener las password cifradas para el acceso al almacén de certificados recién creado, para ello:
 1. Crear el fichero keypass.cleartext con la password (en claro) empleada para proteger la private key dentro del keystore.

2. Crear el fichero storepass.cleartext con la password (en claro) para el acceso al keystore.
 3. Cifrar los ficheros anteriores con el comando ampasword proporcionado en el apartado 5.2.1 Instalación Administration Tools

```
$ ./ampasword --encrypt keypass.cleartext > .keypass
$ ./ampasword --encrypt storepass.cleartext > .storepass
```
 4. Eliminar los ficheros keypass.cleartext y storepass.cleartext
 5. Copiar los ficheros .keystore, .keypass y .storepass en todos los nodos.
3. Reiniciar todos los servidores de aplicaciones para que recojan los cambios.

Para obtener más información acceda a la guía de administración del producto:

<http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/admin-guide/index/chap-certs-keystores.html> apartado 19.3

El Certificado de Firma de Componentes debe ser generado y configurado correctamente para la puesta en producción.

5.3.2 Creación del IPD para el dominio de correo.

1. Acceder a la consola de administración web de openam, pestaña “Tareas Comunes”



2. Dar de alta un nuevo Proveedor de identidades alojado.

Se mostrará una nueva ventana donde se deberán indicar los parámetros para el nuevo IDP.



Servicio de WebSSO
Manual de instalación y configuración

**Consejería de Economía,
Innovación y Ciencia**



Servicio de WebSSO Manual de instalación y configuración

Consejería de Economía,
Innovación y Ciencia

VERSION: 1.0.0 CERRAR SESION

Usuario: amAdmin Servidor: prucorss01

OpenAM

Crear un proveedor de identidades de SAMLv2 en este servidor

Esta página permite configurar esta instancia de servidor OPENSAML como proveedor de identidades (IDP). Puede proporcionar un nombre para el proveedor, círculo de confianza (COT), sus metadatos del proveedor y, opcionalmente, un certificado de firma. Un círculo de confianza (COT) es un grupo de proveedores de identidades (IDP) y proveedores de servicios (SP) que confían mutuamente y, en realidad, representa los confines en los que se realizan todas las comunicaciones de la federación. Los metadatos representan la configuración necesaria para ejecutar protocolos de federación (p.ej. SAMLv2), además del mecanismo para comunicar esta configuración a otras entidades (p.ej. SP) en un COT. Generaremos los metadatos si no tiene ninguno. Debe seleccionar un dominio para este proveedor si hay más de uno en el sistema. De lo contrario, este proveedor se configurará bajo el dominio raíz.

* Indica que el campo es obligatorio

¿Tiene metadatos para este proveedor?: ☐ Sí ☒ No

metadatos

* Dominio:

* Nombre:

Clave para firmar:

Círculo de confianza

Seleccione uno de la lista de círculos de confianza existentes o proporcione uno para crearlo e incluir en él este IDP. Un círculo de confianza (COT) es un grupo de proveedores de identidades (IDP) y proveedores de servicios (SP) que confían mutuamente y representan los confines en los que se realizan todas las comunicaciones de SAMLv2.

* Nuevo círculo de confianza:

Asignación de atributos

La asignación de atributos ayuda a garantizar que tanto el proveedor de servicios (SP) como el proveedor de identidades (IDP) puedan reconocer los mismos atributos que puedan tener nombres exclusivos. Por ejemplo, el SP puede tener un atributo denominado UserName, pero el IDP puede llamarlo UserID. La eliminación de estas inconsistencias mediante la asignación de los atributos garantizará que los datos se transfieran correctamente.

Asignación de atributos

Los parámetros que hay que introducir son los siguientes:

- ¿tiene metadatos para este proveedor?: NO
- Dominio: correo
- Nombre: URL completa del balanceador de OpenAM, indicando https y con la URI /opensso
Ejemplo: https://ssoweb.des.i-administracion.junta-andalucia.es/opensso
- Clave para firma: Seleccione la clave creada en el apartado anterior.
- New Circle Of Trust: cot_correo

3. Definir el Mapeo de atributos. Será necesario definir los campos devueltos por defecto dentro de la aserción SAML para este dominio.

Acceder a la pestaña "Federación" y en la sección de "Proveedores de Identidades" editar el IDP recién creado.



Servicio de WebSSO Manual de instalación y configuración

Consejería de Economía,
Innovación y Ciencia

| | | | | | |
|----------------|-------------------|------------|---------------|---------------|----------|
| Tareas comunes | Control de acceso | Federación | Servicios web | Configuración | Sesiones |
|----------------|-------------------|------------|---------------|---------------|----------|

Configuración del círculo de confianza Configuración de SAML 1.x

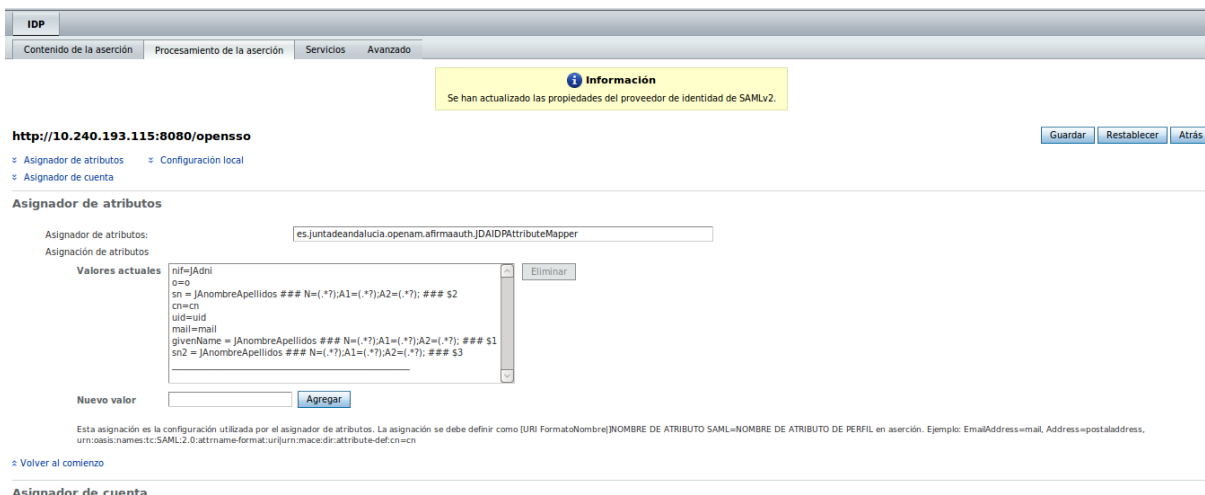
Configuración del círculo de confianza

Esta sección se puede utilizar para configurar las propiedades del círculo de confianza. La tabla de entidades se puede utilizar para administrar los proveedores de entidades, incluida la importación y la exportación de proveedores. Las entidades se pueden agregar al círculo de confianza una vez creadas en la tabla de entidades.

| Círculo de confianza (2 Elemento(s)) | | | |
|--------------------------------------|--------|--|---------|
| Nuevo... Eliminar | | | |
| <input type="checkbox"/> | Nombre | Entidades | Dominio |
| <input type="checkbox"/> | correo | pruebaCorreo saml2 qqqqqqqqqqqqqqqqqqqqqqqqqqqqqq saml2 http://10.240.193.115:8080/opensso saml2 | /correo |
| <input type="checkbox"/> | guia | pruebaCorreo saml2 http://10.240.193.115:8080/opensso saml2 | /guia |

| Proveedores de identidades (5 Elemento(s)) | | | | | |
|--|------------------------------------|-----------|--------------------------|-----------|---------|
| Nuevo... Eliminar Importar entidad... | | | | | |
| <input type="checkbox"/> | Nombre | Protocolo | Tipo | Ubicación | Dominio |
| <input type="checkbox"/> | http://10.240.193.115:8080/opensso | SAMLv2 | IDP | Alojado | /correo |
| <input type="checkbox"/> | http://10.240.193.115:8080/opensso | SAMLv2 | IDP | Alojado | /guia |
| <input type="checkbox"/> | pruebaCorreo | SAMLv2 | SP: XACML PEP; AttrQuery | Remoto | /guia |
| <input type="checkbox"/> | pruebaCorreo | SAMLv2 | SP: XACML PEP; AttrQuery | Remoto | /correo |
| <input type="checkbox"/> | qqqqqqqqqqqqqqqqqqqqqqqqqqqqqq | SAMLv2 | SP: XACML PEP; AttrQuery | Remoto | /correo |

Acceder a la pestaña “Procesamiento de la aserción”



The screenshot shows the WebSSO configuration interface. At the top, there is a navigation bar with tabs: 'IDP', 'Contenido de la aserción', 'Procesamiento de la aserción', 'Servicios', and 'Avanzado'. Below the navigation bar, there is a yellow information box stating: 'Se han actualizado las propiedades del proveedor de identidad de SAMLv2.' Below this, the URL 'http://10.240.193.115:8080/opensso' is displayed. There are three buttons: 'Guardar', 'Restablecer', and 'Atrás'. Below the URL, there are two links: 'Asignador de atributos' and 'Configuración local'. Below these links, there is a section titled 'Asignador de atributos'. In this section, there is a text input field containing 'es.juntadeandalucia.openam.afirmaauth.JDAIDPAttributeMapper'. Below this field, there is a list of 'Valores actuales' (current values) with an 'Eliminar' button next to it. The list contains the following items: 'nif=JAdni', 'o=o', 'sn = JAnombreApellidos ### N=(.?.);A1=(.?.);A2=(.?.); ### \$2', 'cn=cn', 'uid=uid', 'mail=mail', 'givenName = JAnombreApellidos ### N=(.?.);A1=(.?.);A2=(.?.); ### \$1', and 'sn2 = JAnombreApellidos ### N=(.?.);A1=(.?.);A2=(.?.); ### \$3'. Below the list, there is a 'Nuevo valor' (new value) input field and an 'Agregar' button. At the bottom, there is a small note: 'Esta asignación es la configuración utilizada por el asignador de atributos. La asignación se debe definir como URI FormatoNombre(NOMBRE DE ATRIBUTO SAML=NOMBRE DE ATRIBUTO DE PERFIL en aserción. Ejemplo: EmailAddress=mail, Address=postaladdress, urn:oasis:names:tc:SAML:2.0:attribute-format:urn:urn:mace:dir:attribute-def:cn=cn'.

En el campo “Asignador de Atributos” poner el valor:

`es.juntadeandalucia.openam.afirmaauth.JDAIDPAttributeMapper`

Nota: Esto activará un mapeador de atributos generado dentro del proyecto, el cual permite definir atributos basados en expresiones regulares. Para más detalle de este generador y su uso ir al correspondiente anexo dentro de este documento.

En el apartado “Asignador de atributos” introducir las siguientes entradas:

- uid=uid
- givenName = JAnombreApellidos ### N=(.?.);A1=(.?.);A2=(.?.); ### \$1
- sn = JAnombreApellidos ### N=(.?.);A1=(.?.);A2=(.?.); ### \$2
- sn2 = JAnombreApellidos ### N=(.?.);A1=(.?.);A2=(.?.); ### \$3
- nif=JAdni
- mail=mail
- o=o

5.3.3 Creación del IPD para el dominio GUIA.

1. Acceder a la consola de administración web de openam, pestaña Tareas comunes



2. Dar de alta un nuevo Proveedor de identidades alojado.

Se mostrará una nueva ventana donde se deberán indicar los parámetros para el nuevo IDP. Los parámetros que hay que introducir son los siguientes:

- ¿tiene metadatos para este proveedor?: NO
- Dominio: guia.
- Nombre: URL completa del balanceador de OpenAM, indicando https y con la URI /opensso
Ejemplo: <https://ssoweb.des.i-administracion.junta-andalucia.es/opensso>
- Clave para firma: Seleccione la clave creada en el apartado anterior.
- New Circle Of Trust: cot_guia



Servicio de WebSSO Manual de instalación y configuración

Consejería de Economía,
Innovación y Ciencia

VERSION: 1.0.0
Usuario: amAdmin Servidor: prucorss01 CERRAR SESION

OpenAM

Crear un proveedor de identidades de SAMLv2 en este servidor

Esta página permite configurar esta instancia de servidor OPENSOURCE como proveedor de identidades (IDP). Puede proporcionar un nombre para el proveedor, círculo de confianza (COT), sus metadatos del proveedor y, opcionalmente, un certificado de firma. Un círculo de confianza (COT) es un grupo de proveedores de identidades (IDP) y proveedores de servicios (SP) que confían mutuamente y, en realidad, representa los confines en los que se realizan todas las comunicaciones de la federación. Los metadatos representan la configuración necesaria para ejecutar protocolos de federación (p.ej. SAMLv2), además del mecanismo para comunicar esta configuración a otras entidades (p.ej. SP) en un COT. Generaremos los metadatos si no tiene ninguno. Debe seleccionar un dominio para este proveedor si hay más de uno en el sistema. De lo contrario, este proveedor se configurará bajo el dominio raíz.

* Indica que el campo es obligatorio

¿Tiene metadatos para este proveedor?: ☐ Sí ☒ No

metadatos

* Dominio:

* Nombre:

Clave para firmar:

Círculo de confianza

Seleccione uno de la lista de círculos de confianza existentes o proporcione uno para crearlo e incluir en él este IDP. Un círculo de confianza (COT) es un grupo de proveedores de identidades (IDP) y proveedores de servicios (SP) que confían mutuamente y representa los confines en los que se realizan todas las comunicaciones de SAMLv2.

* Nuevo círculo de confianza:

Asignación de atributos

La asignación de atributos ayuda a garantizar que tanto el proveedor de servicios (SP) como el proveedor de identidades (IDP) puedan reconocer los mismos atributos que puedan tener nombres exclusivos. Por ejemplo, el SP puede tener un atributo denominado UserName, pero el IDP puede llamarlo UserID. La eliminación de estas inconsistencias mediante la asignación de los atributos garantizará que los datos se transfieran correctamente.

Asignación de atributos

3. Definir el Mapeo de atributos. Será necesario definir los campos devueltos por defecto dentro de la aserción SAML para este dominio.

Acceder a la pestaña “Federación” y en la sección de “Proveedores de Identidades” editar el IDP recién creado.

Tareas comunes Control de acceso Federación Servicios web Configuración Sesiones

Configuración del círculo de confianza Configuración de SAML 1.x

Configuración del círculo de confianza

Esta sección se puede utilizar para configurar las propiedades del círculo de confianza. La tabla de entidades se puede utilizar para administrar los proveedores de entidades, incluida la importación y la exportación de proveedores. Las entidades se pueden agregar al círculo de confianza una vez creadas en la tabla de entidades.

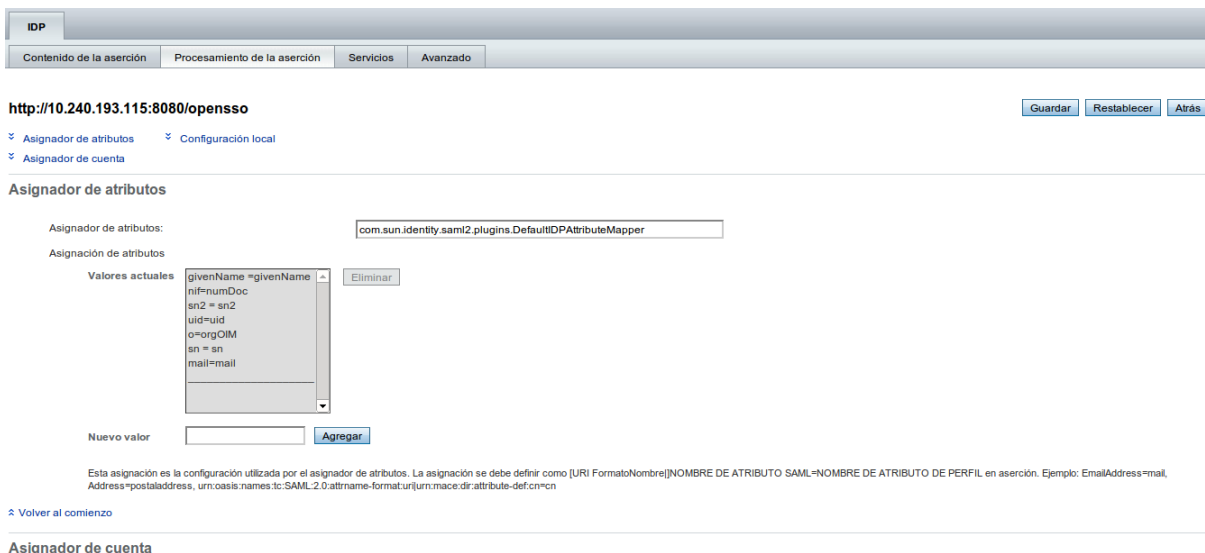
Círculo de confianza (2 Elemento(s))

| Nombre | Entidades | Dominio | Estado |
|---------------------------------|---|---------|--------|
| <input type="checkbox"/> correo | pruebaCorreo[saml2] http://10.240.193.115:8080/opensso/saml2 | /correo | Activo |
| <input type="checkbox"/> guía | pruebaCorreo[saml2] http://10.240.193.115:8080/opensso/saml2 | /guia | Activo |

Proveedores de identidades (5 Elemento(s))

| Nombre | Protocolo | Tipo | Ubicación | Dominio |
|---|-----------|--------------------------|-----------|---------|
| <input type="checkbox"/> http://10.240.193.115:8080/opensso | SAMLv2 | IDP | Alojado | /correo |
| <input type="checkbox"/> http://10.240.193.115:8080/opensso | SAMLv2 | SP | Alojado | /guia |
| <input type="checkbox"/> pruebaCorreo | SAMLv2 | SP: XACML PEP; AttrQuery | Remoto | /correo |
| <input type="checkbox"/> pruebaCorreo | SAMLv2 | SP: XACML PEP; AttrQuery | Remoto | /correo |
| <input type="checkbox"/> pruebaCorreo | SAMLv2 | SP: XACML PEP; AttrQuery | Remoto | /correo |

Acceder a la pestaña “Procesamiento de la aserción”



The screenshot shows the 'IDP' configuration page with the 'Procesamiento de la aserción' tab selected. The URL is `http://10.240.193.115:8080/opensso`. There are buttons for 'Guardar', 'Restablecer', and 'Atrás'. Below the tabs, there are links for 'Asignador de atributos', 'Configuración local', and 'Asignador de cuenta'. The 'Asignador de atributos' section shows the current value `com.sun.identity.saml2.plugins.DefaultIDPAttributeMapper` and a list of attributes: `givenName = givenName`, `nif=numDoc`, `sn2 = sn2`, `uid=uid`, `o=orgOIM`, `sn = sn`, and `mail=mail`. There is an 'Eliminar' button next to the list. Below the list, there is a 'Nuevo valor' field and an 'Agregar' button. A note at the bottom states: 'Esta asignación es la configuración utilizada por el asignador de atributos. La asignación se debe definir como [URI FormatoNombre][NOMBRE DE ATRIBUTO SAML=NOMBRE DE ATRIBUTO DE PERFIL en aserción. Ejemplo: EmailAddress=mail, Address=postaladdress, urn:oasis:names:tc:SAML:2.0:attribute-format:uriurn:mace:dir:attribute-def:cn=cn]'. There is a link 'Volver al comienzo'.

En el campo “Asignador de Atributos” **dejar el valor por defecto, al contrario que el IDP asignado a correo, en el IDP de GUIA NO es necesario procesar ningún atributo basado en expresiones regulares.**

En el apartado “Asignador de atributos” introducir las siguientes entradas:

- uid=uid
- givenName =givenName
- sn = sn
- sn2 = sn2
- nif=numDoc
- mail=mail
- o=orgOIM

6 Servidores Secundarios de OpenAM

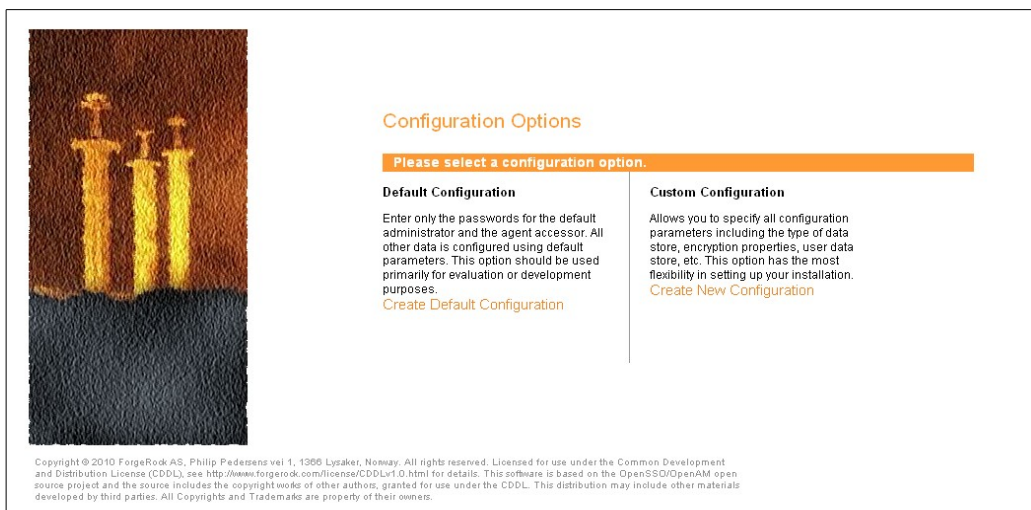
Una vez instalado y configurado el servidor primario de Openam, puede proceder a configurar los servidores secundarios.

Para ello, deberá primero verificarse que se ha realizado la instalación del software base en el servidor secundario, tal como se indica en el punto 4. Instalación del software base.

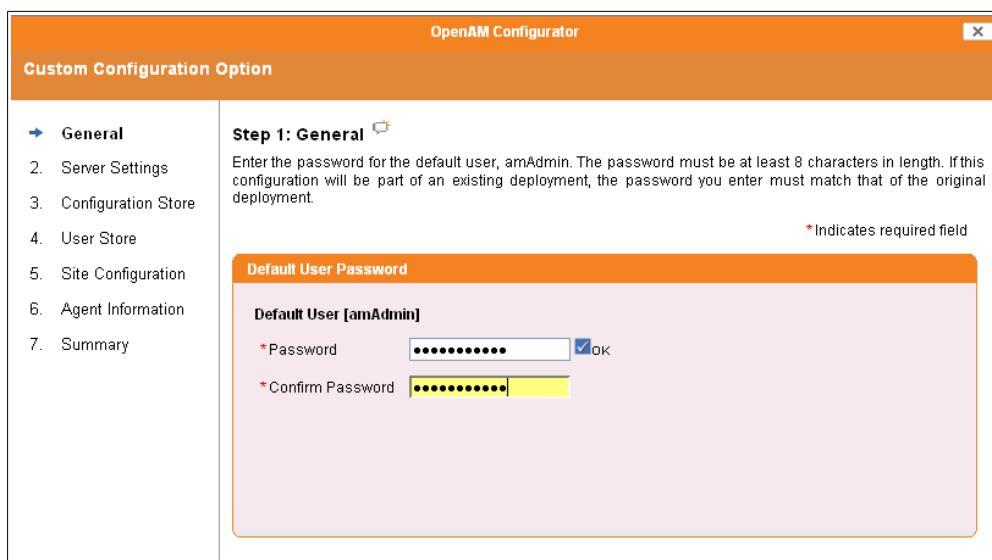
Esta configuración deberá realizarse por cada uno de los nodos secundarios que se desee instalar.

Para configurar un nodo secundario se deberá seguir los siguientes pasos:

1. Acceder mediante un navegador web a la URL de la consola de administración del nodo de OpenAM:
`https://<nombre_completo_servidorN>:[ssl_port]/opensso/console`
2. Se mostrará la página web de inicio de configuración del producto:

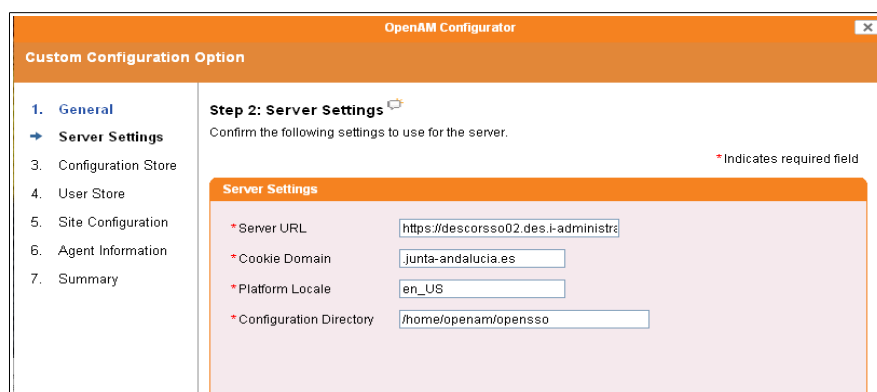


3. Pulsar en “Create New Configuration...”; se mostrará la primera página del OpenAM Configurator. Introducir la contraseña del administrador de la consola amadmin. Si la contraseña cumple los requisitos de calidad (8 caracteres mínimo, incluyendo minúsculas y mayúsculas), se mostrará un botón de OK a la derecha de la contraseña. Una vez introducida la contraseña y la confirmación, pulsar en “Next”.



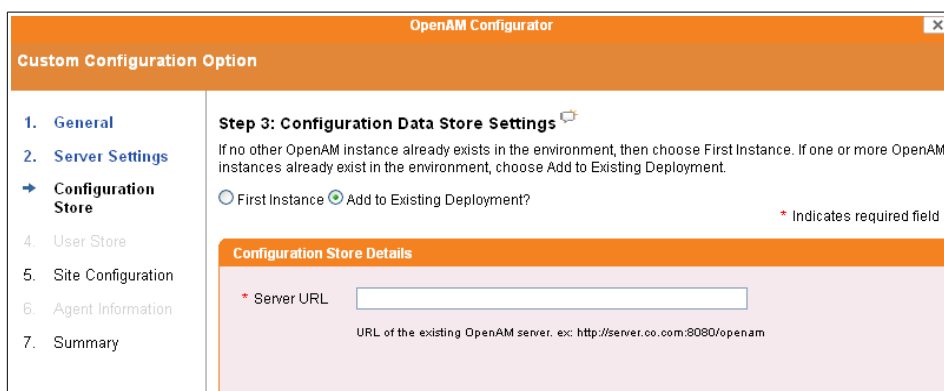
4. En la ventana de configuración del servidor, especificar los parámetros de configuración de OpenAM:
- Server URL: FQDN del **segundo servidor** de OpenAM, especificando **https** y el puerto seguro
 - Dominio de la cookie de autenticación (incluyendo el punto inicial): **.junta-andalucia.es**
 - Localización de la plataforma: **es_ES**
 - Directorio local de configuración de OpenAM: **/home/openam/opensso**

Una vez introducidos estos datos, pulsar **Next** para continuar.

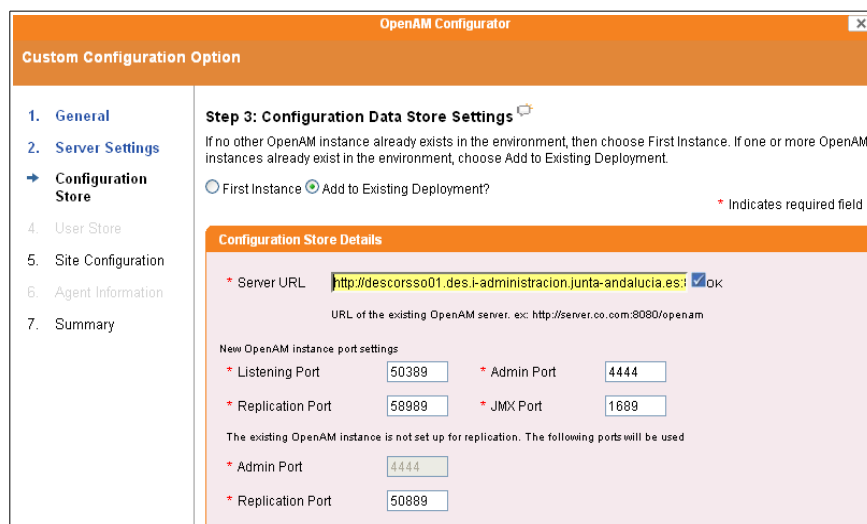


5. En la siguiente ventana, el asistente web de configuración solicitará los

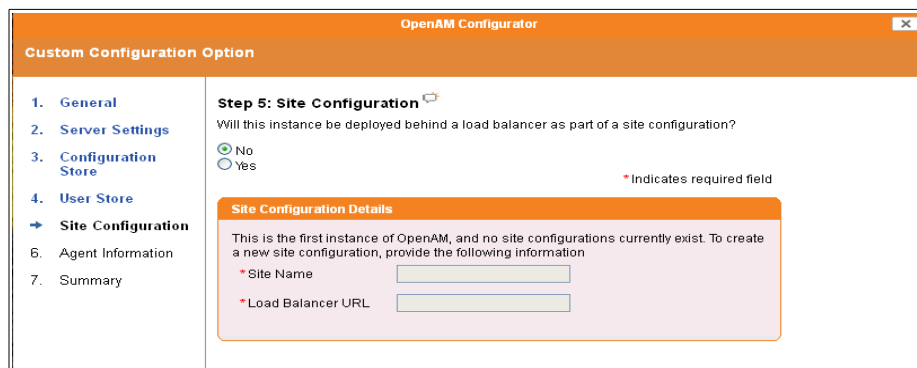
datos del repositorio de datos (OpenDS embebido). Indicar que se va a añadir a un despliegue ya existente, marcando la opción **“Add to existing deployment”**, y en la URL que se solicita, indicar la URL del primer nodo de OpenAM (especificando http y puerto 8080, y terminando en /openso):



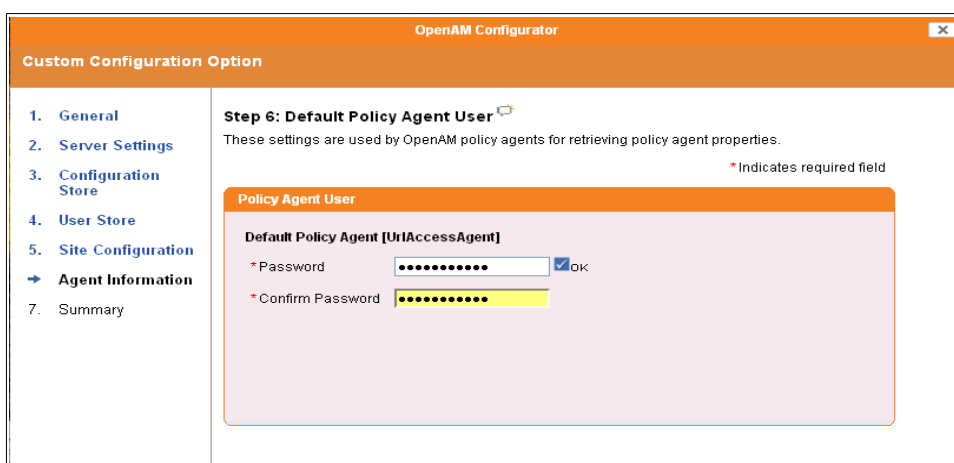
6. El configurador detectará automáticamente la información de OpenAM del primer servidor, mostrando los puertos correspondientes (no hay que modificarlos). Copiar el dato contenido en **“Encryption Key”**. A continuación pulsar **Next**:



7. En el paso **5.Site Configuration**, marcar **No** y pulsar **Next** (la configuración del clúster se realizará desde la administración de OpenAM).

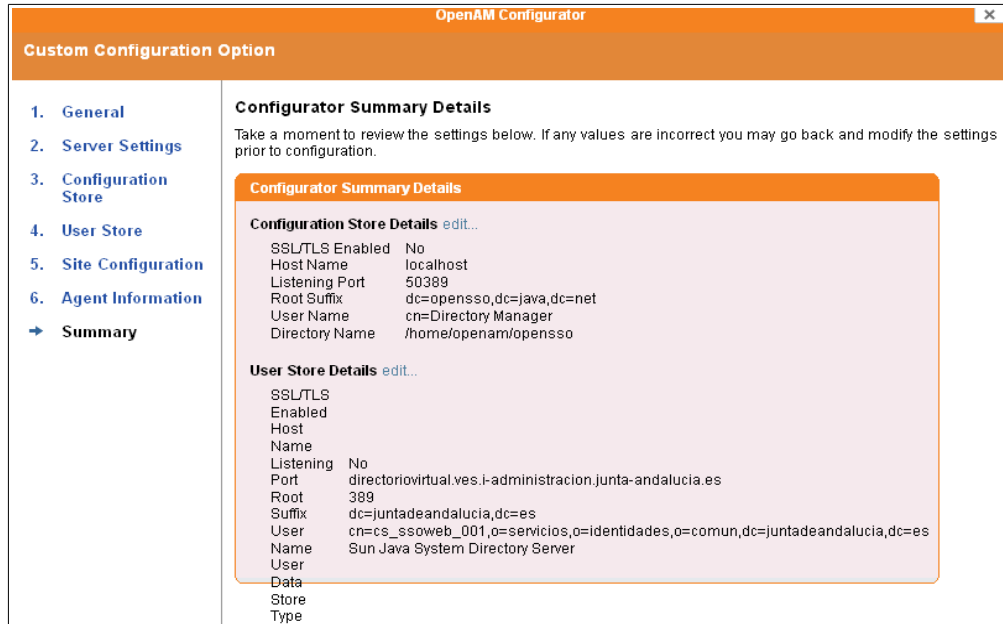


The screenshot shows the 'OpenAM Configurator' window at 'Step 5: Site Configuration'. The left sidebar lists steps 1 through 7, with 'Site Configuration' (step 5) highlighted. The main content area asks 'Will this instance be deployed behind a load balancer as part of a site configuration?' with radio buttons for 'No' (selected) and 'Yes'. Below this, a 'Site Configuration Details' box contains a message: 'This is the first instance of OpenAM, and no site configurations currently exist. To create a new site configuration, provide the following information'. It includes two required fields: '* Site Name' and '* Load Balancer URL', both with empty text input boxes. A red asterisk indicates required fields.



The screenshot shows the 'OpenAM Configurator' window at 'Step 6: Default Policy Agent User'. The left sidebar lists steps 1 through 7, with 'Agent Information' (step 6) highlighted. The main content area asks 'These settings are used by OpenAM policy agents for retrieving policy agent properties.' Below this, a 'Policy Agent User' box contains a message: 'Default Policy Agent [UrlAccessAgent]'. It includes two required fields: '* Password' and '* Confirm Password', both with masked text input boxes. An 'OK' button is next to the password field. A red asterisk indicates required fields.

8. En la última ventana del asistente web, se mostrará un resumen de la configuración. Revisar la configuración, y pulsar en **“Create Configuration”** para realizar la configuración del producto:



OpenAM Configurator

Custom Configuration Option

- 1. General
- 2. Server Settings
- 3. Configuration Store
- 4. User Store
- 5. Site Configuration
- 6. Agent Information
- ➔ Summary

Configurator Summary Details

Take a moment to review the settings below. If any values are incorrect you may go back and modify the settings prior to configuration.

Configurator Summary Details

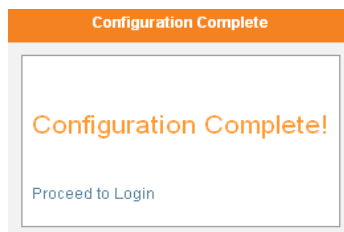
Configuration Store Details [edit...](#)

| | |
|-----------------|---------------------------|
| SSL/TLS Enabled | No |
| Host Name | localhost |
| Listening Port | 50389 |
| Root Suffix | dc=opensso,dc=java,dc=net |
| User Name | cn=Directory Manager |
| Directory Name | /home/openam/opensso |

User Store Details [edit...](#)

| | |
|-----------------|--|
| SSL/TLS Enabled | No |
| Host Name | directoriovirtual.ves.i-administracion.junta-andalucia.es |
| Listening Port | 389 |
| Root Suffix | dc=juntadeandalucia,dc=es |
| User Name | cn=cs_ssoweb_001,o=servicios,o=identidades,o=comun,dc=juntadeandalucia,dc=es |
| User Name | Sun Java System Directory Server |
| Data Store Type | |

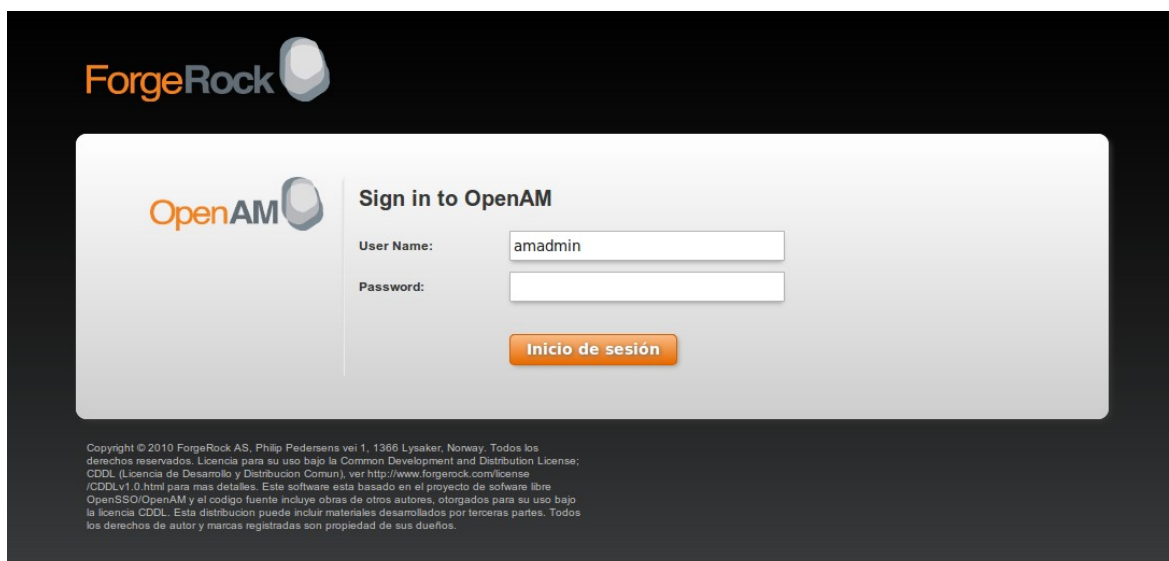
9. Si la configuración se realiza correctamente, se mostrará un mensaje de configuración completada. Pulsar en **Proceed to login** para autenticarse a la consola de OpenAM.



Configuration Complete

Configuration Complete!

[Proceed to Login](#)



ForgeRock

OpenAM

Sign in to OpenAM

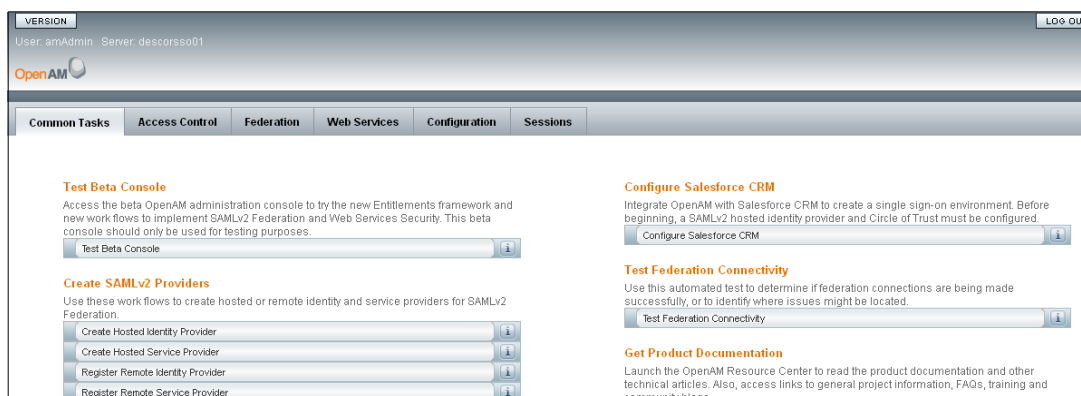
User Name:

Password:

Inicio de sesión

Copyright © 2010 ForgeRock AS. Philip Pedersens vei 1, 1366 Lysaker, Norway. Todos los derechos reservados. Licencia para su uso bajo la Common Development and Distribution License; CDDL (Licencia de Desarrollo y Distribución Común), ver <http://www.forgerock.com/licenses/CDDLv1.0.html> para más detalles. Este software está basado en el proyecto de software libre OpenSSO/OpenAM y el código fuente incluye obras de otros autores, otorgados para su uso bajo la licencia CDDL. Esta distribución puede incluir materiales desarrollados por terceras partes. Todos los derechos de autor y marcas registradas son propiedad de sus dueños.

10. Si la autenticación se realiza correctamente, se mostrará la consola de administración de OpenAM:



7 Configuración del clúster de OpenAM

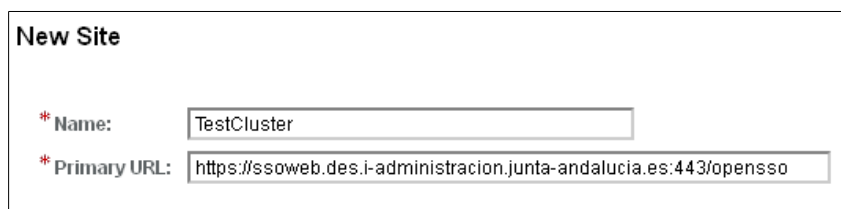
7.1 Añadir nodos secundarios al cluster

Una vez instalado el software base en los nodos secundarios, estos deben configurarse y añadirse al clúster de OpenAM. Para realizar esta configuración deben seguirse los pasos que se indican a continuación:

1. Acceder mediante un navegador web a la URL de administración del servidor secundario de OpenAM:
https://<nombre_completo_servidorN>:[ssl_port]/opensso
2. Pulsar en la pestaña “**Configuration**”
3. Pulsar en la pestaña “**Servers and Sites**”.
4. Se mostrará un listado de los servidores de OpenAM incluidos en esta configuración. Como se puede observar en la configuración, están dados de alta los dos servidores de OpenAM, con sus respectivas URLs.



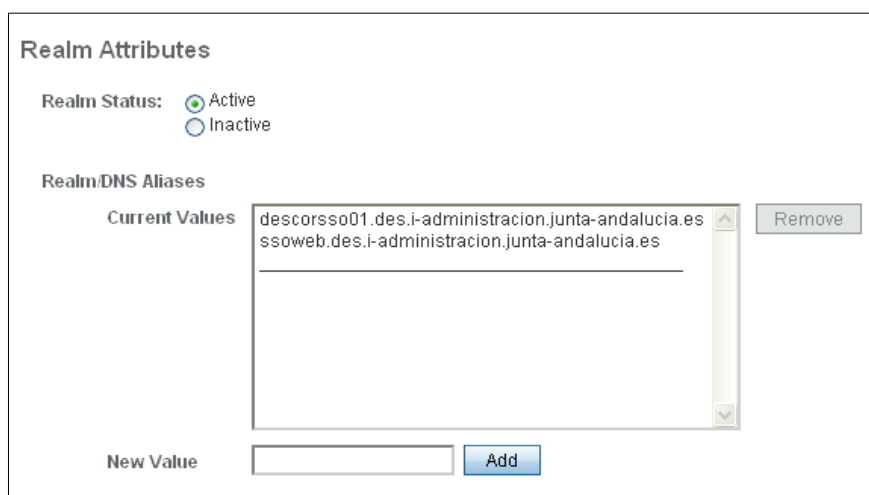
5. En la sección “**Sites**”, pulsar en “**New...**”
6. En la siguiente ventana (“**New Site**”), indicar un nombre descriptivo del Site, y la URL del balanceador (especificando **https**, puerto **443**, y terminando en **/opensso**). Al terminar pulsar en **OK**.



7. En la ventana “**Servers and Sites**”, en la sección “**Sites**” se habrá añadido el nuevo Site de OpenAM, y como Primary URL aparecerá la del balanceador:



8. Pulsar en la pestaña **“Access Control”**, y a continuación pulsar en el enlace del Realm (**Top: Level Realm**).
9. Verificar que está añadido el balanceador en el parámetro **“Realm/DNS Aliases”**.



10. Pulsar **“Back to Access Control”**, a la derecha de la ventana, y luego en las pestañas **“Configuration”** y **“Servers and Sites”**.
11. En la sección **“Servers”**, pulsar en el primer servidor de la lista:



12. Se mostrará una ventana con los detalles de configuración para ese servidor. En la lista desplegable etiquetada como **“Parent Site”**, seleccionar el nombre del sitio bajo el cual estará este servidor:

Edit https://descorss01.des.i-administracion.junta-andalucia.es:8443/opensso

Inheritance Settings

Site Debugging
System Mail Server

Site

Parent Site:

Back to top TestCluster

13. Una vez asignado al site, pulsar en **Save**, en la parte derecha de la ventana. Cuando se muestre el mensaje “**Information: Server profile was updated**”, pulsar en “**Back to servers and sites**”.

14. En la ventana de “**Servers and sites**” se puede observar que el primer servidor está asignado al sitio indicando anteriormente:

Servers and Sites

Default Server Settings

Servers (2 Item(s))

New ... Delete Clone ...

| Server Name | Site Name |
|---|-------------|
| <input checked="" type="checkbox"/> https://descorss01.des.i-administracion.junta-andalucia.es:8443/opensso | TestCluster |
| <input type="checkbox"/> https://descorss02.des.i-administracion.junta-andalucia.es:8443/opensso | |

15. Repetir el paso anterior con el segundo servidor de OpenAM.

16. Al final del proceso, los dos servidores de OpenAM tienen que estar asignados al sitio, y en la información del sitio se puede verificar que tiene los dos servidores asignados (**Assigned Servers**):

Servers and Sites

Default Server Settings

Servers (2 Item(s))

New ... Delete Clone ...

| Server Name | Site Name |
|---|-------------|
| <input checked="" type="checkbox"/> https://descorss01.des.i-administracion.junta-andalucia.es:8443/opensso | TestCluster |
| <input type="checkbox"/> https://descorss02.des.i-administracion.junta-andalucia.es:8443/opensso | TestCluster |

Sites (1 Item(s))

New ... Delete

| Site Name | Primary URL | Assigned Servers |
|---|--|--|
| <input checked="" type="checkbox"/> TestCluster | https://ssoweb.des.i-administracion.junta-andalucia.es:443/opensso | https://descorss01.des.i-administracion.junta-andalucia.es:8443/opensso https://descorss02.des.i-administracion.junta-andalucia.es:8443/opensso |

17. Pulsar en **Log Out** para salir de la consola de administración, en la parte superior derecha de la ventana.

7.2 Instalación del balanceador de sesiones

En el siguiente apartado se detalla el procedimiento para realizar la configuración

del failover de sesiones:

8. Acceder mediante SSH y con usuario **openam** al primer servidor Linux donde se ha desplegado OpenAM.
9. Definir la variable de entorno del JRE, editando con VI el fichero de perfil del usuario (**/home/openam/.bash_profile**), y añadiendo la siguiente línea al final de este fichero:

export JAVA_HOME=/opt/software/jdk1.6.X/

10. Cargar el perfil del usuario **openam**, con el comando: **source /home/openam/.bash_profile**
11. Copiar el fichero **"/tools/ssoSessionUtils.zip"** en el directorio **/home/openam/**
12. Cambiar los permisos de ejecución del fichero **ssoSessionUtils.zip** a 750, y propietario **openam**:

```
[root@descorss01 openam]# chown openam:openam ssoSessionUtils.zip
[root@descorss01 openam]# chmod 750 ssoSessionUtils.zip
-rwxr-x--- 1 openam openam 74450948 abr 10 10:19 ssoSessionTools.zip
```

13. Cambiar la sesión al usuario **openam**, y descomprimir el fichero **"ssoSessionUtils.zip"** con **unzip**, directamente en el directorio **/home/openam/**

unzip ssoSessionUtils.zip

14. Ejecutar el script **./setup.sh** con usuario **openam**, en el directorio temporal donde se copió.

```
[root@descorss01 ssoSessionTools]# ./setup
Name of the directory to install the scripts (example: sfoscripts):sfoscripts
The scripts are properly setup under directory: /home/openam/sfoscripts
JMQ is properly setup under directory /home/openam/sfoscripts/jmq
```

15. Una vez instalados los scripts, eliminar el fichero **/home/openam/ssoSessionUtils.zip**
16. Con usuario **openam**, y posicionarse en el siguiente directorio: **/home/openam/jmq/imq/bin**
17. Editar con VI el fichero **/home/openam/jmq/imq/etc/imqenv.conf**, y añadir la siguiente línea al final del fichero:

IMQ_DEFAULT_JAVAHOME=/opt/software/jdk1.6.X

18. Guardar y cerrar el fichero.

19. Ejecutar el siguiente comando: `./imqbrokerd -name aminstance -port 7777 &`

```
[openam@descorso01 bin]$ ./imqbrokerd -name aminstance -port 7777 &
[1] 11385
[openam@descorso01 bin]$ [04/abr/2012:17:39:43 CEST]
=====
=====
Sun GlassFish(tm) Message Queue 4.4
Sun Microsystems, Inc.
Version: 4.4 (Build 16-a)
Compile: Thu Aug 27 07:43:07 PDT 2009

Copyright (c) 2009 Sun Microsystems, Inc. All rights reserved. Use is
subject to license terms.
=====
=====
Java Runtime: 1.6.0_25 Sun Microsystems Inc. /opt/software/jdk/jre
[04/abr/2012:17:39:43 CEST] IMQ_HOME=/home/openam/jmq/jmq/imq
[04/abr/2012:17:39:43 CEST] IMQ_VARHOME=/home/openam/jmq/jmq/imq/var
[04/abr/2012:17:39:43 CEST] Linux 2.6.18-92.el5 amd64 descorso01 (2 cpu) openam
[04/abr/2012:17:39:43 CEST] Java Heap Size: max=188416k, current=188416k
[04/abr/2012:17:39:43 CEST] Arguments: -name aminstance -port 7777
[04/abr/2012:17:39:43 CEST] [B1060]: Loading persistent data...
[04/abr/2012:17:39:43 CEST] Using built-in file-based persistent store:
/home/openam/jmq/jmq/imq/var/instances/aminstance/
[04/abr/2012:17:39:44 CEST] [B1039]: Broker "aminstance@descorso01:7777" ready.
```

20. Una vez que el broker está arrancado, pulsar ENTER para salir de la ventana de arranque.

21. Verificar que el broker está escuchando peticiones en el puerto 7777, con el comando **netstat**:

```
[openam@descorso01 bin]$ netstat -an | grep 7777

tcp      0      0 :::7777          :::*              LISTEN
```

22. Añadir al broker un usuario llamado **user**, con el comando "**imqusermgr**":

```
[openam@descorso01 bin]$ ./imqusermgr add -u user -g admin -p password -i
aminstance

User repository for broker instance: aminstance
User user successfully added.
```

Donde **<user>** es el nombre del usuario que se va a crear para el broker, **<admin>** es el grupo donde va a crear (por defecto admin), y **<password>** es la contraseña de este usuario.

23. Editar con VI el fichero **/home/openam/sfoscripts/config/lib/amsfo.conf** y añadir las siguientes líneas:

```
CLUSTER_LIST=<nombre_completo_servidor1>:7777,<nombre_completo_servidor2>:7777
```

Donde:

<nombre_completo_servidor1>: es el FQDN del primer servidor Linux.

<nombre_completo_servidor2>: es el FQDN del segundo servidor Linux.

24. Modificar también las siguientes líneas:

```
BROKER_INSTANCE_NAME=<nombre_instancia_broker>  
DATABASE_DIR="/home/openam/jmq/db/sessiondb"  
LOG_DIR="/home/openam/jmq/logs"  
USER_NAME=user
```

Donde **<nombre_instancia_broker>** es el nombre que se indicó en el arranque del broker (por ejemplo, aminstance).

25. Guardar y cerrar el fichero.

26. Crear con usuario openam los directorios **/home/openam/jmq/db/sessiondb**, y **/home/openam/jmq/logs**

27. Posicionarse en el directorio **/home/openam/sfoscripts/bin**

28. Ejecutar el comando: **./amsfopassword -f /home/openam/sfoscripts/.password -e password**

```
[openam@descorss01 bin]$ ./amsfopassword -f /home/openam/mqpwd.txt -e password  
  
os.name=Linux  
CON EXITO
```

Donde **<password>** es la contraseña de conexión al broker

29. Posicionarse en el directorio **/home/openam/jmq/imq/bin**

30. Reiniciar los componentes del servicio de failover, mediante el siguiente comando:

```
[openam@descorss01 bin]$ ./imqcmd shutdown bkr -b localhost:7777  
  
Username: user (usuario que se especificó en el punto 18)  
Password: password (contraseña que se especificó en el punto 18)  
Shutting down the broker specified by:  
  
-----  
Host Primary Port
```

```
-----  
localhost 7777
```

```
Are you sure you want to shutdown this broker? (y/n)[n] y
```

```
Waiting for broker at localhost:7777 to shutdown...  
Successfully shutdown the broker.
```

31. Posicionarse en el directorio **/home/openam/sfoscripts/bin**

32. Arrancar la instancia del broker, con el siguiente comando: **./amsfo start**

33. Verificar que el broker está escuchando peticiones en el puerto 7777, con el comando **netstat**:

```
[openam@descorso01 bin]$ netstat -an | grep 7777
```

```
tcp      0      0 :::7777          :::*              LISTEN
```

34. Repetir los pasos anteriores en el segundo servidor de Linux. En el paso 19, el parámetro **CLUSTER_LIST** debe quedar con el orden de los servidores a la inversa, primero el segundo servidor:

```
CLUSTER_LIST=<nombre_completo_servidor2>:7777,<nombre_completo_servidor1>:7777
```

7.3 Configuración del balanceo de sesiones en OpenAM

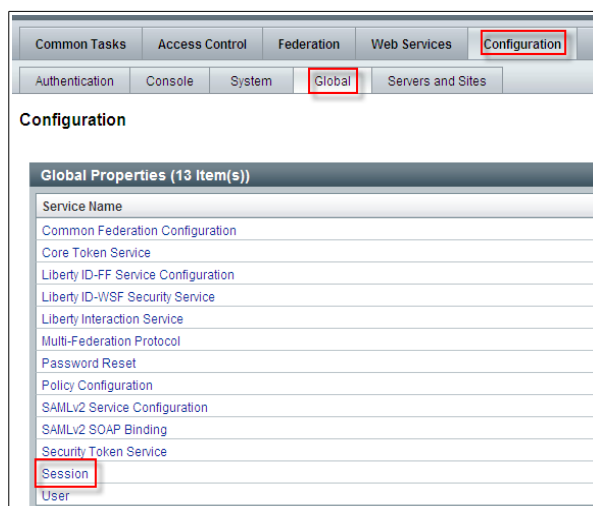
Para terminar la configuración del balanceo de sesiones en la infraestructura, será necesario completar las siguientes tareas de configuración desde la consola de OpenAM:

1. Mediante un navegador web, acceder a la URL del balanceador de la consola de OpenAM (especificando **https**), y autenticarse con el usuario **amadmin**

NOTA: es necesario acceder a la URL del balanceador, no a la de los nodos específicos, por ejemplo:

<https://ssoweb.des.i-administracion.junta-andalucia.es/opensso>

2. Pulsar en la pestaña “**Configuration**” y a continuación pulsar en la pestaña “**Global**”.
3. En los enlaces que se muestran, pulsar en “**Session**”:



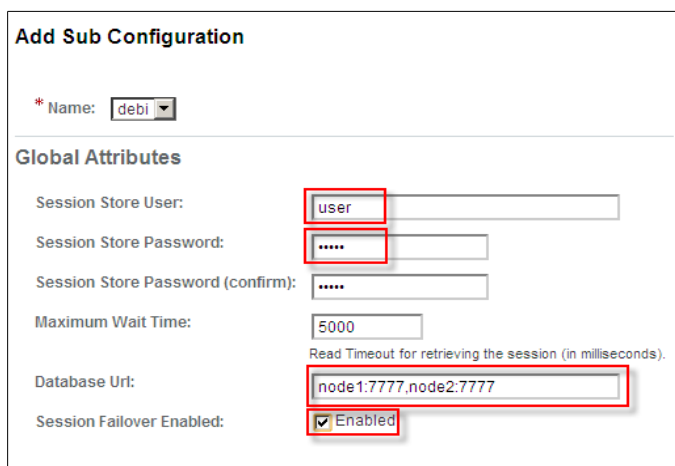
4. En la siguiente ventana, pulsar en **“New”**, para añadir una instancia de configuración:

Secondary Configuration Instance



5. Se mostrará la ventana **“Add Sub Configuration”**. Indicar los siguientes parámetros:

- Name: nombre del clúster (Site) de OpenAM
- Session Store User: usuario de conexión la base de datos de sesiones
- Session Store Password/confirm: contraseña del usuario de conexión de la base de datos de sesiones.
- Maximum Wait Time: 500
- Database URL:
nombre_completo_servidor1:7777,nombre_completo_servidor2:7777
- Session Failover Enabled: marcada (para habilitar el failover de sesiones)



Add Sub Configuration

* Name:

Global Attributes

Session Store User:

Session Store Password:

Session Store Password (confirm):

Maximum Wait Time:

Read Timeout for retrieving the session (in milliseconds).

Database Url:

Session Failover Enabled: ☒ Enabled

6. Pulsar en **"Add"**.
7. Pulsar en **Save**.
8. Pulsar en **"Back to Server Configuration"**.
9. Detener el message broker (**./amsfo stop**) y el Tomcat de cada servidor.
10. Reiniciar el message broker (**./amsfo start**) y el Tomcat del primer servidor Linux.
11. Reiniciar el message broker (**./amsfo start**) y el Tomcat del segundo servidor Linux.

8 Anexos

8.1 Depuración de errores.

Openam guarda los logs del sistema bajo en dos directorios opensso/debug y opensso/log localizados bajo el directorio de configuración (ver apartado 5.1 Configuración de la instancia principal de OpenAM punto 5 -Directorio local de configuración de OpenAM).

El módulo de autenticación desarrollado bajo el proyecto escribe su log en el archivo opensso/debug/Afirma.

El nivel de log, puede ser establecido desde la consola de administración, para ello acceda a la consola de administración.

`https://<servidor_ssoweb>:[ssl_port]/opensso/console`

Acceda a la pestaña configuración-> Servidores y acceda al servidor que dese configurar.



En la sección de Depuración puede cambiar el nivel de log (opción nivel de depuración) al valor que se estime adecuado.

Para reportar errores se recomienda poner durante las pruebas los servidores en el nivel mensaje.



Servicio de WebSSO Manual de instalación y configuración

Consejería de Economía,
Innovación y Ciencia

⚙ Sistema ⚙ Servidor de correo

Sitio

Sitio principal:

[Volver al comienzo](#)

Sistema

Directorio base de instalación:
El directorio base en el que residen los datos del producto. (nombre de la propiedad: com.planet.services.configpath)

Configuración regional predeterminada:
La configuración regional predeterminada del producto. (nombre de la propiedad: com.planet.am.locale)

URL de notificación:
La ubicación del punto final del servicio de notificación. Normalmente, se trata del URL/servicio de notificación de la implementación del producto. (nombre de la propiedad: com.sun.identity.client.notification.url)

Validación de XML:
Especifica si es necesaria la validación cuando se analizan documentos XML. (nombre de la propiedad: com.planet.am.util.xml.validating)

[Volver al comienzo](#)

Depuración

Nivel de depuración:
El nivel de depuración de todos los componentes del producto. (nombre de la propiedad: com.planet.services.debug.level)

Combinar archivos de depuración:
On: dirige todos los datos de depuración a un archivo único (debug.out); Off: crea archivos de depuración separados por componentes (nombre de propiedad: com.sun.services.debug.mergeall)

Directorio de depuración:
El directorio en el que residen los archivos de depuración. (nombre de la propiedad: com.planet.services.debug.directory)

[Volver al comienzo](#)

8.2 Mapeador de Atributos JDAIDPAttributeMapper

Openam posee un mapeador de atributos muy básico, el cual sólo permite generar atributos en base a campos presente en el datastore, pero sin permitir la modificación o preprocesamiento del valor de estos campos. Para suplir esa limitación y poder generar atributos cuyo valor incluya un preprocesado y composición basado en expresiones regulares, se ha desarrollado en el proyecto un mapeador de atributos denominado JDAIDPAttributeMapper.

Este mapeador detecta atributos definidos según el siguiente patrón:

```
CAMPO_DEVUELTO = CAMPO_ORIGEN ### EXPRESION_REGULAR_ORIGEN ###  
PATRON_VALOR_DESTINO
```

Para explicar su funcionamiento lo mejor es poner un ejemplo.

El directorio de correo define un atributo llamado JAnombreApellidos que contiene el nombre y apellidos de una cuenta de correo según el siguiente formato.

N=NOMBRE;A1=APELLIDO1;A2=APELLIDO2;

Para poder procesar la cadena anterior, extrayendo cada uno de los elementos que la compone y poder así generar cadenas con formatos distintos, se puede emplear el mapeador de atributos del proyecto, definiendo por ejemplo la siguiente cadena.

usuario = JAnombreApellidos ### N=(.*?);A1=(.*?);A2=(.*?); ### \$2 \$3, \$1

La cadena anterior define un nuevo atributo “usuario” cuyo valor se obtiene tras procesar el campo JAnombreApellidos presente en el datastore. El procesamiento

incluye una primera expresión regular, $N=(.*?);A1=(.*?);A2=(.*?);$ que será empleada para procesar el valor del campo JAnombreApellidos ($N=NOMBRE;A1=APELLIDO1;A2=APELLIDO2;$) y extraer cada uno de los elementos que la compone (nombre, apellido1 y apellido2). La ultima expresión regular define la cadena resultante (\$2 \$3, \$1), en este caso produciría una salida formada por APELLIDO1 APELLIDO2, NOMBRE.

Si tuviésemos una entrada JAnombreApellidos con el valor $N=Juan;A1=Español;A2=Europeo;$ el mapeador generaría el siguiente resultado:

usuario = Español Europeo, Juan.

Otros ejemplos:

Extraer el nombre del usuario del campo JAnombreApellidos y asignarlo a un nuevo atributo GivenName:

GivenName = JAnombreApellidos ### $N=(.*?);A1=(.*?);A2=(.*?);$ ### \$1

Extraer el primer apellido del usuario del campo JAnombreApellidos y asignarlo a un nuevo atributo sn:

sn = JAnombreApellidos ### $N=(.*?);A1=(.*?);A2=(.*?);$ ### \$2

Extraer el segundo apellido del usuario del campo JAnombreApellidos y asignarlo a un nuevo atributo sn2:

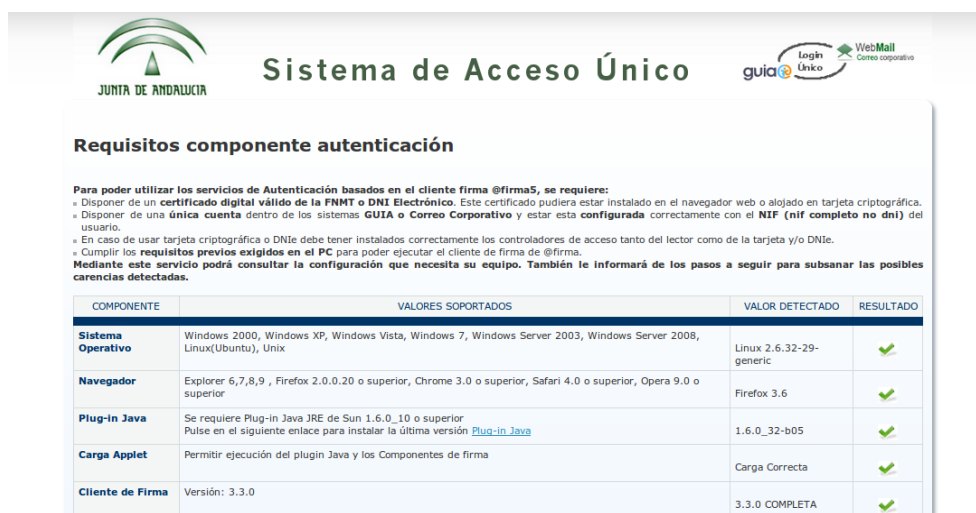
sn2 = JAnombreApellidos ### $N=(.*?);A1=(.*?);A2=(.*?);$ ### \$3

8.3 Página de Verificación del componente de autenticación por certificados.



Dentro de la página de login, el enlace “¿Problemas? Verificar Requisitos” lleva a la aplicación de verificación de Requisitos para la ejecución del componente de firma de @firma, necesario para realizar el login por certificados.

Si los usuario del sistema tienen problemas en la carga del applet de @firma, a la hora de realizar los proceso de autenticación de usuario, se deberá remitir al mismo a dicha página para que realice la verificación de sus sistema mediante esta aplicación.



Requisitos componente autenticación

Para poder utilizar los servicios de Autenticación basados en el cliente firma @firma5, se requiere:

- » Disponer de un **certificado digital válido de la FNMT o DNI Electrónico**. Este certificado pudiera estar instalado en el navegador web o alojado en tarjeta criptográfica.
- » Disponer de una **única cuenta** dentro de los sistemas **GUIA o Correo Corporativo** y estar esta **configurada** correctamente con el **NIF (nif completo no dni)** del usuario.
- » En caso de usar tarjeta criptográfica o DNte debe tener instalados correctamente los controladores de acceso tanto del lector como de la tarjeta y/o DNte.
- » Cumplir los **requisitos previos exigidos en el PC** para poder ejecutar el cliente de firma de @firma.

Mediante este servicio podrá consultar la configuración que necesita su equipo. También le informará de los pasos a seguir para subsanar las posibles carencias detectadas.

| COMPONENTE | VALORES SOPORTADOS | VALOR DETECTADO | RESULTADO |
|--------------------------|--|-------------------------|-----------|
| Sistema Operativo | Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Linux(Ubuntu), Unix | Linux 2.6.32-29-generic | ✓ |
| Navegador | Explorer 6,7,8,9 , Firefox 2.0.0.20 o superior, Chrome 3.0 o superior, Safari 4.0 o superior, Opera 9.0 o superior | Firefox 3.6 | ✓ |
| Plug-in Java | Se requiere Plug-in Java JRE de Sun 1.6.0_10 o superior Pulse en el siguiente enlace para instalar la última versión Plug-in Java | 1.6.0_32-b05 | ✓ |
| Carga Applet | Permitir ejecución del plugin Java y los Componentes de firma | Carga Correcta | ✓ |
| Cliente de Firma | Versión: 3.3.0 | 3.3.0 COMPLETA | ✓ |



Servicio de WebSSO
Manual de instalación y configuración

**Consejería de Economía,
Innovación y Ciencia**

La personalización de dicha aplicación puede realizarse editando los ficheros contenidos en la ruta : [ruta_tomcat_ssoweb]/webapps/opensso/jda/RequisitosAE

8.4 Urls.

A continuación se incluyen un resumen de urls:

Consola de administración:

[https://\[url_ssoweb\]\[:ssl_port\]/opensso/console](https://[url_ssoweb][:ssl_port]/opensso/console)

Login directo en dominio correo:

[https://\[url_ssoweb\]\[:ssl_port\]/opensso/UI/Login](https://[url_ssoweb][:ssl_port]/opensso/UI/Login)

[https://\[url_ssoweb\]\[:ssl_port\]/opensso/UI/Login?realm=correo](https://[url_ssoweb][:ssl_port]/opensso/UI/Login?realm=correo)

Login directo en dominio guía:

[https://\[url_ssoweb\]\[:ssl_port\]/opensso/UI/Login?realm=guia](https://[url_ssoweb][:ssl_port]/opensso/UI/Login?realm=guia)

Metadatos del IDP asociado al dominio correo:

[https://\[url_ssoweb\]\[:ssl_port\]/opensso/saml2/jsp/exportmetadata.jsp?realm=/correo](https://[url_ssoweb][:ssl_port]/opensso/saml2/jsp/exportmetadata.jsp?realm=/correo)

Metadatos del IDP asociado al dominio guía:

[https://\[url_ssoweb\]\[:ssl_port\]/opensso/saml2/jsp/exportmetadata.jsp?realm=/guia](https://[url_ssoweb][:ssl_port]/opensso/saml2/jsp/exportmetadata.jsp?realm=/guia)