Checklist de Instalación de IdP y/o SP.

Preparado para:	**Proyecto CONFIA**
Preparado por:	**Yaco Sistemas S.L.**
Versión:	2
Fecha:	25/05/2010
Ref. YACO:	P174MAN090968

Yaco Sistemas S.L. Inscrita en el Registro Mercantil de Sevilla, tomo 3.496 de Sociedades,

Control de Versiones del Documento			
Versión	**Fecha**	**Descripción del Cambio**	**Autor**
1	15/08/09	Versión inicial	S. Martín
2	25/05/10	Versión final	S. Martín

Índice de contenido

1.- Introducción

Una vez que tengamos instalado y configurado un IdP, un SP o ambos, hay una serie de comprobaciones que debemos seguir para que todo nos funcione correctamente. Si aún no hemos instalado ni configurado las herramientas lo ideal es visitar el documento de la federación https://trac.yaco.es/confia/wiki/GuiadeInstalacion o directamente la web de simplesamlphp http://rnd.feide.no/content/installing-simplesamlphp

2.- Checklist

- ✔ **IdPs y Sps sincronizados**

  En la federación tanto los IdPs como los SPs deben de estar sincronizados. Para ello lo mas fácil es instalar un servicio de NTP (Net Time Protocol) para que la hora de los elementos de la federación se sincronice.

- ✔ **Existe en la carpeta de configuración de Simplesamlphp un archivo config.php**

  Si no es así copiarlo de una plantilla existente en config-templates y configurarlo.

- ✔ **Existe en la carpeta de configuración de Simplesamlphp un archivo authsources.php**

  Si no es así copiarlo de una plantilla existente en config-templates y configurarlo.
  - En el caso de un IdP deberemos establecer las fuentes de autenticación.
  - En el caso de un SP deberemos de establecer las fuentes SP (metadatos de cada SP que queramos configurar)

- ✔ **En el caso de IdP existe en la carpeta de metadatos de Simplesamlphp un archivo con los metadatos del IdP. (saml20-idp-hosted.php)**

  Si no es así copiarlo de una plantilla existente en metadata-templates y configurarlo. Vía navegador puede comprobarse que los metadatos están bien configurados accediendo a la pestaña 'federación' a los enlaces de 'Ver Metadatos' de las entidades.

- ✔ **Existe en la carpeta de metadatos archivos donde se definen los metadatos de los IdP/SP con los que queremos conectarnos**

  Si no es así no se alarme, la federación automáticamente importa estos metadatos de IdP/SP remotos si el módulo de metarefresh está bien configurado.
  Asegurase que en el archivo de configuración de simplesamlphp (config/config.php) tiene convenientemente definida la variable 'metadata.sources'.

- ✔ **En la carpeta que contiene los metadatos que importa el módulo metarefresh tiene permisos de escritura el servidor que corre el IdP/SP**

  Si no es así darle permisos de escritura, de lo contrario al ejecutar el metarefresh dará un error.

- ✔ **Compruebe que los módulos metarefresh y cron estén activos**

  Para comprobar si el modulo está activo puede comprobarse:
  - Viendo si existe un archivo enable o (default-enable y no hay disable) dentro del directorio del módulo (estará en modules/nombre_modulo/)
  - Vía navegador en la pestaña 'configuración' y pulsando sobre 'Available modules'.

- ✔ **Está la configuración del módulo de metarefresh convenientemente configurada**

  Compruebe que en la carpeta config existe el archivo config-metarefresh.php y está convenientemente configurado. Si no es asi tiene una plantilla dentro del direcotorio config-templates del módulo metarefresh.
  Para comprobar que está bien configurada acceda vía navegador a su IdP/SP y en la pestaña 'federación' pulse sobre el enlace que ejecutara el refresco de los metadatos 'Metarefresh: fetch metadata'.
  Sino ha dado ningún error se habrán creado ficheros con los metadatos de las entidades remotas. Puede ver los metadatos bién mirando los ficheros o accediendo vía navegador a la pestaña 'federación', acceder como administrador y ya aparecerán tanto las entidades locales como las remotas.

- ✔ **Está correctamente configurado el módulo del cron para que se importen los metadatos**

  Compruebe que en la carpeta config existe el archivo module_cron.php y está convenientemente configurado. Si no es asi tiene una plantilla dentro del directorio config-templates del módulo cron.
  Para comprobar que el cron está bien configurado acceda vía navegador a su IdP/SP y en la pestaña 'configuración' pulse sobre el enlace 'Cron module information page'

- ✔ **Esta correctamente habilitado el cron en el sistema**

  Compruebe que el crontab del /etc/cron.d está correctamente configurado y que en el tiempo que está definido se producen las actualizaciones de los metadatos.

- ✔ **En el caso de haber necesitado configurar filtros, comprobarlos.**

  Compruebe que los filtros se están ejecutando correctamente, tenga en cuenta que los filtros se definen en diferentes sitios por lo que puede que unos filtros entren en conflicto con otros ya sea porque estén duplicados o porque se están ejecutando en un orden erroneo.

- ✔ **En el caso de que se trate de un IdP comprobar que las fuentes de autenticación funcionan correctamente.**

  Vía navegador acceda a la pestaña 'Autenticación' del IdP, pulse sobre la fuente de autenticación que quiera comprobar e introduzca las credenciales en el formulario. (Asegurase de que en el caso de fallar no se trate de problemas con las credenciales). Si todo ha ido bien accederá a una vista donde se muestran los datos del usuario autenticado.

- ✔ **Compruebe que los metadatos de la entidad están dados de alta en la federación y los metadatos y los certificados son válidos.**

  Acceder vía navegación al Gestor de metadatos a la pestaña 'federación' y acceder al enlace 'Validador de entidades de Janus' y comprobar que nuestra entidad aparece y ha sido validada correctamente.

- ✔ **En el caso de que se trate de un IdP ver si se está suministrado a la federación los datos que necesita.**

  Existe en el WAYF de la federación un mecanismo para comprobarlo.
  Para ello acceda vía navegador al WAYF a la pestaña 'federación' y acceda al enlace 'Módulo de validación de atributos'. Se le mostrará una vista donde podrá seleccionar su IdP y autenticarse trás lo cual se le mostrará un informe detallado de si los datos suministrados son válidos y suficientes o no.
  En el caso de que el IdP no aparezca en la lista, contacte con los administradores de la federación pues su entidad no está dada de alta en el Gestor de Metadatos y por tanto el WAYF no conoce su entidad.

- ✔ **En el caso de que se trate de un SP comprobar que puede autenticar contra un IdP de la federación.**

  Vía navegador acceda a la pestaña 'Autenticación' del IdP, pulse sobre la fuente de autenticación saml que quiera comprobar, seleccione un IdP que sepa que funciona, meta las credenciales y compruebe que accede a una vista donde se muestran los datos del usuario logado y que los datos son los esperados.

- ✔ **Comprobar que en la maquina existe un servidor de correos.**

  Tanto los IdP como los SP necestan poder enviar correos ya que utilizan este sistema para reportar errores, permitir contacto entre usuario-administrador y avisar de posibles problemas detectados tras la monotorización del sistema.

3.- Más información de interés

Instalación de SimpleSAMLphp:
http://confia.aupa.info/trac/wiki/Documentacion/InstalacionSimpleSAMLphp

Guía de instalación de un IdP:
http://confia.aupa.info/trac/wiki/Documentacion/GuiaIdP

Guía de instalación de un SP
http://confia.aupa.info/trac/wiki/Documentacion/GuiaSP

Integración en el gestor de metadatos de CONFIA:
http://confia.aupa.info/trac/wiki/Documentacion/IntegracionSimpleSAMLphpGestorMetadatosCONFIA

Filtros de procesamiento de atributos en simpleSAMLphp
http://confia.aupa.info/trac/wiki/Documentacion/FiltrosAtributos

Preguntas frecuentes:
http://confia.aupa.info/trac/wiki/Documentacion/FAQ

Configuración de la arquitectura Hub And Spoke con simpleSAMLphp
http://confia.aupa.info/trac/wiki/Documentacion/ConfiguracionHubAndSpoke