Dedícale tiempo a…

…actualizar el IdP de referencia

José Manuel Macías Luna
https://redir.is/macias

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Red IRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

¿a qué llamamos IdP de referencia?

- … a un software concreto (SimpleSAMLphp) que reúne todos los requisitos para participar como IdP en SIR2
- Permite, entre otras posibilidades:
  - integrarse con distintos repositorios de identidad (directorios, bases de datos relacionales, sistemas de single-sign-on como CAS o ADFS,…)
  - poder establecer reglas de emisión de atributos de una manera flexible
  - ¡podemos hacer muchas otras cosas!
- Y además:
  - de código abierto
  - con una comunidad detrás

Buenas prácticas...

- Al menos deberíamos disponer de dos entornos: pre-producción, y producción
- Idealmente podrían ser hasta *4* entornos (DTAP):
  - Development → Desarrollo
  - Testing → Pruebas
  - Acceptance → Aceptación de pruebas
  - Production → Producción
- El entorno en el que provemos antes de pasar a producción debe ser lo más parecido posible al de producción

Buenas prácticas... (II)

- Conviene tener separados:
  - el software en sí (incluyendo módulos que extiendan funcionalidad)
  - las configuraciones
  - los datos
  - las personalizaciones de aspecto que hagamos
- Conviene NO:
  - hacer modificaciones directamente sobre el código base
- Es muy recomendable:
  - Disponer de un repositorio con control de cambios

Buenas prácticas... (II)

- Más buenas prácticas incluyen:
  - tener políticas de backup frecuentes
  - no tener depuración activada en producción
  - tener políticas de rotación de logs
  - estar al tanto de actualizaciones de seguridad
  - tener documentados procesos y procedimientos, y también los cambios realizados

SimpleSAMLphp: el software en sí...

- Se distribuye en “releases”
- También *instalable* mediante composer
- Principalmente se distribuye en las siguientes rutas:
  - `lib/` → la mayor parte de la funcionalidad
  - `modules/` → módulos que extienden funcionalidad
  - `www/` → interfaz web pública
- Otras rutas, relacionadas con el software:
  - `attributemap/` → mapeos de atributos
  - `dictionaries/` → traducciones
  - `docs/` → documentación
  - `schemas/` → esquemas SAML
  - `vendor/` → librerías de terceros

Configuraciones en SimpleSAMLphp

- Principalmente los ficheros:
  - `config/config.php`
  - `config/authsources.php`
  - `metadata/saml20-idp-hosted.php`
  - `metadata/saml20-sp-remote.php`
- Como referencia, podemos usar siempre las plantillas que encontraremos en:
  - `config-templates` y `metadata-templates`

"datos" en SimpleSAMLphp

- Dentro de esta categoría podríamos incluir:
  - el repositorio de datos, que suele ser remoto
  - los certificados, que se guardan en `cert/`
  - los logs, que encontraremos en `logs/` (salvo si hemos configurado `syslog`)

Personalización de aspecto en SimpleSAMLphp

- Conviene no hacer modificaciones sobre www/
- La forma correcta de modificar el aspecto en SimpleSAMLphp es mediante temas:
  - +información: https://redir.is/CWVKM~
- Nota: se está trabajando en la inclusión de un nuevo sistema de plantillas para la versión 1.17 de SimpleSAMLphp, basado en Twigg
- Las traducciones son otra forma de personalizar mensajes, pero es conveniente trabajar/contribuir con las traducciones oficiales, ya que son la forma de mantener coherencia entre versiones

Algunas notas sobre seguridad

- Poner una contraseña de administrador robusta
  - En `config.php` → `'auth.adminpassword'`
- El salt del IdP debería parecer un salt
  - En `config.php` → `'secretsalt'`
- Proteger índice del IdP con administrador:
  - En `config.php` → `'admin.protectindexpage'`

Ejercicio 1:

- Configuraremos nuestro entorno de pruebas, para ello, descargaremos Docker (si no lo tenemos) y seguiremos las instrucciones de este enlace:
  - https://redir.is/78KQX~
- Los que quieran trabajar sobre su propio entorno y ya tengan desplegado un IdP, pueden ir averiguando como ejercicio cual es la versión de SimpleSAMLphp instalada…

Ejercicio 2:

- En la imagen Docker, vamos a probar un proveedor de servicio ya instalado, está aquí:
  - https://sp.dedicaletiempoa.rediris.es/sp/

  (los datos del usuario configurado están en el fichero del ejercicio anterior)
- Cuando hayáis accedido, quiero que guardéis la respuesta obtenida. Podéis pegar el contenido de dicha respuesta.
- Acceded al interfaz de administración del IdP, y comprobad la versión instalada

Ejercicio 3:

- Vamos a actualizar el IdP, para ello:
  - haremos copia de seguridad del IdP actual
  - descargaremos release más actual: https://simplesamlphp.org/download
  - en config copiaremos `config.php` y `authsources.php` de nuestra copia de seguridad
  - en `modules/`, copiaremos el módulo que aporta el tema del IdP, que está en `modules/sir2skin` de nuestro backup
  - en `metadata/`, copiaremos todos los archivos que teníamos en el directorio del mismo nombre de nuestro backup
  - en `cert/` copiaremos el certificado del IdP
- Borrad cookies, probad a autenticaros de nuevo al SP inicial y comparad la respuesta ¿son iguales?

Ejercicio 4:

- Repasad las recomendaciones de seguridad de la slide 10 (algunas notas sobre seguridad) sobre el nuevo IdP
- ¿hay opciones que se puedan considerar inseguras en la configuración?
- Realizad algún cambio sobre el tema `modules/sir2skin` para personalizar el aspecto del IdP

Ejercicio 5.

- En el contenedor tenemos instalado composer.
- Realizar la instalación de SimpleSAMLphp según el procedimiento descrito en esta página:

https://simplesamlphp.org/docs/stable/simplesamlphp-install-repo

- ¿es equivalente a la instalación desde una release?

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares