Inserta el logotipo de tu institución

Federación de identidades

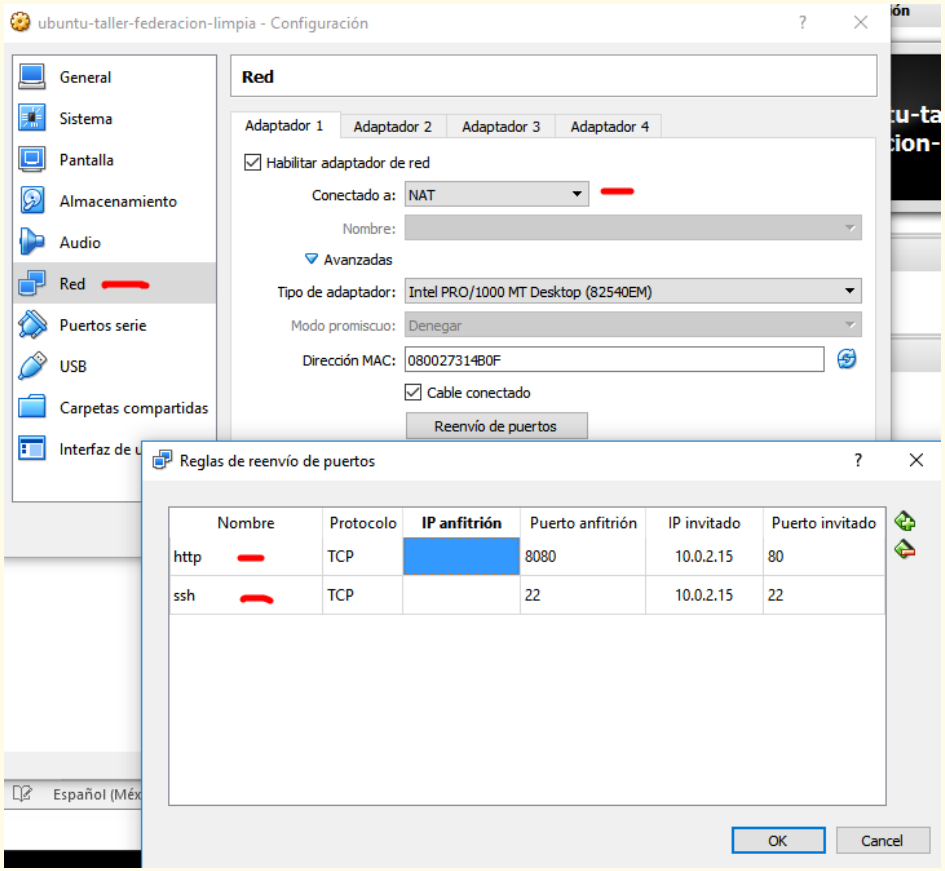
Fernando Aranda – CUDI, A.C.
Juan Gabriel Cruz Pérez - UCOL

Puerto Vallarta, Jalisco, del 29 de mayo al 02 de junio

Preparando el servidor

Importar máquina virtual

Preparar redirección de puertos (*si es requerido*)



Iniciando

- Datos de acceso (linux y mysql)
  - Usuario:federacion
  - Clave: federacion
- Paquete Simplesamlphp en /var/www

Pasos iniciales

Descomprimir el paquete simplesaml

*/var/www$***sudo tar -xvzf simplesamlphp-1.14.14.tar.gz**

Renombrar carpeta

sudo mv simplesamlphp-1.14.14 simplesamlphp

Crear alias en apache

- Abrir: */etc/apache2/sites-enabled/000-default.conf*
- Ubicar *DocumentRoot*
- Agregar la siguiente línea

  Alias */simplesaml /var/www/simplesamlphp/www*

Guardar

Reiniciar apache: *service apache2 restart*

Probar instalación

Ingresar a la carpeta alias que se acaba de crear.

Configuración básica

Cambiar password administración
Cambiar secretsalt

Creando certificado

Crear carpeta

/var/www/simplesamlphp/cert/

Ejecute los siguientes comandos:

openssl genrsa -out IP.key 1024

openssl req -new -key IP.key -out IP.csr

openssl x509 -req -days 1825 -in IP.csr -signkey IP.key -out IP.crt

Configurando el sp

Dirijase a la carpeta

/var/www/simplesamlphp/config/

Abra el archivo authsources.php

Elimine todo el contenido

Agregue el siguiente source:

```
<?php
$config = array(
        'curso-sp' => array(
            'saml:SP',
            'entityID' => 'http://participanteN',
            'idp' => null,
             'certificate' => 'IP.crt',
            'privatekey' => 'IP.key',
        ),
);
```

Revise los metadatos en su navegador

IDP remoto

Dirijase a carpeta /var/www/simplesamlphp/metadata/

Elimine todos los archivos cuyo nombre no inicien con saml

Abra el archivo saml20-idp-remote.php

Pegue los metadatos del IDP de pruebas.

Probando el sp

A través de su navegador ingrese a la carpeta simplesaml de su servidor.

Seleccione pestaña autenticación

Haga clic en la opción “Probar las fuentes para la autenticación ya configuradas”.

Haga clic en el source curso-sp.

Ingrese datos de acceso:

Usuario:curso

Clave:curso

Eliminar la selección de idp

Abra el archivo config/authsources.php
Cambie el atributo idp a ‘idp-curso’
Inicie sesión nuevamente.

Usando una aplicación demo.

- Dirijase a la carpeta /var/www/html/demo/
- Verifique que los valores de las variables en config.php coincidan con su instalación.
- En su navegador, vaya a la carpeta raiz de su servidor.
- Inicie sesión

Configurando el IDP

- Copie la carpeta simplesamlphp a una carpeta llamada *idp*
- En la configuración de apache agregue un alias para el idp
- Reinicie apache
- Abra el archivo config.php de la carpeta idp/config/, sustituya el valor para la variable *baseurlpath* por 'idp/' y cambie a true el valor de la variable *enable.saml20-idp*. Guarde los cambios
- Abra el archivo authsources.php y elimine el source existente.
- Verifique el acceso a la carpeta idp desde su navegador.

Creando usuarios

Cree la base de datos Usuario y una tabla usuario con campos: id, nombre, correo y clave, agregue al menos un registro.

Creando source para el idp

- Abra el archivo config-templates/authsources.php
- Busque el source example-sql
- Copie el contenido y peguelo en config/authsources.php
- Haga los siguientes cambios:

  Nombre source: idp-curso

  'dsn' => 'mysql:host=localhost;port=3306;dbname=Usuarios,
  'username'='federacion'
  'password'='federacion'
  'query'='select id,correo,nombre from usuarios where correo=:*username* and clave=:*password*',
- Guarde los cambios.
- Desde su navegador verifique que permite autenticarse.

Creando metadatos para el idp

- Abra el archivo metadata/saml20-idp-hosted.php
- Cambie el indice '_DYNAMIC:1_' por su nombre.
- Cambie los valores privatekey y certificate por los certificados creados previamente.
- Cambie el valor de auth por el el nombre del source creado recientemente para el idp.
- Elimine los atributos y comentarios restantes.
- Verifique desde su navegador los metadatos en la pestaña **federación**

Conectando los servicios

En la carpeta de SP, agregue los metadatos de su IDP y viceversa.
Pruebe nuevamente la aplicación demo.

Interconectando IDPS y SP’s

Cada servidor debe aceptar inicios de sesión de cada IDP de los participantes.

wayf (where are you from)

- “Puente” para enlazar y administrar las conexiones entre proveedores de servicios y de identidad.
- Permite agregar, eliminar y cambiar atributos.
- Sirve de “traductor” entre distintos protocolos.