Installazione di un SimpleSAMLphp Service Provider su Debian-Linux
+
Upgrade

28 Gennaio 2015

Autore: Marco Malavolti

Indice generale

1 Introduzione

Questo documento ha lo scopo di guidare l'utente nell'installazione di un Service Provider SimpleSAMLphp su Debian Linux.

2 Software da installare

- openssl
- ntp
- nmap
- apache2
- curl
- cron
- php5 (>=5.3)
- php5-mcrypt
- vim

3 Richiedere il certificato HTTPS per l'SP

a) In linea con le **specifiche tecniche** della Federazione IDEM è necessario installare sulla por- ta 443 un certificato rilasciato da una CA riconosciuta. All'interno della comunità GARR è attivo il servizio di rilascio certificati server denominato **TCS** (TERENA Certificate Service). La caratteristica dei certificati TCS è quella di essere emessi da una CA commerciale che nello specifico consiste in **COMODO CA**.

b) L'elenco delle organizzazioni presso le quali il servizio TCS è già attivo è disponibile in https://ca.garr.it/TCS/tab.php

c) Se il servizio non fosse ancora attivo presso la vostra organizzazione è possibile contattare GARR Certification Service per avviare il procedimento di attivazione
(e-mail a garr-ca@garr.it)

d) Per generare una richiesta di certificato seguire le istruzioni suggerite nelle pagine di documentazione TCS (https://ca.garr.it/TCS/doc_server.php)

Le richieste di certificato devono essere inviate ai referenti TCS presenti nella vostra orga- nizzazione (denominati Contatti Amministrativi TCS). Per conoscere i nomi dei Contatti Amministrativi nominati all'interno del vostro Ente inviare una mail di richiesta a garr-ca@garr.it

4 Modifica del file hosts

Aggiungere al file **/etc/hosts** l'IP, il FQDN e l'Hostname della macchina

scelta per ospitare il Service Provider di SimpleSAMLphp:

```
127.0.1.1 ssp-sp.domain.it ssp-sp
```

5 Installare i pacchetti necessari[1]

a) Eseguire il seguente comando:
- `sudo apt-get install apache2 openssl ntp nmap vim php5 php5-mcrypt curl cron`

b) Aprire le seguenti porte sul/sui firewall:

1) 443 => HTTPS (da e verso la rete internet)

2) 22 => SSH (da e verso l'esterno se vi vuole un controllo remoto)

c) Verificare che sia attivo apache2 e che faccia comparire la pagina "**It Works!**" da **http://ssp-sp.domain.it** o da **http://127.0.1.1**.

[1] per ubuntu 10.04 e superiori

6 Installare SimpleSAMLphp v1.13.2

1) Acquisire i privilegi di ROOT:
   - `sudo su -`
2) Scaricare l'ultima versione del framework SimpleSAMLphp:
   - `cd /opt/`
   - `wget https://simplesamlphp.org/res/downloads/simplesamlphp-1.13.2.tar.gz`
   - `tar xzf simplesamlphp-1.13.2.tar.gz`
   - `mv simplesamlphp-1.13.2 simplesamlphp`
3) Scaricare la Catena di Terena per la validazione del certificato HTTPS della macchina:
   - `mkdir /root/certificates`
   - `wget https://ca.garr.it/mgt/Terena-chain.pem -O /root/certificates/Terena-chain.pem`
4) Modificare il file **/etc/apache2/sites-available/default-ssl** e aggiungere quanto **evidenziato**:

```
DocumentRoot /var/www
Alias /simplesaml /opt/simplesamlphp/www

...

# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
LogLevel debug

...

SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ALL:!aNULL:ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:!MEDIUM

...

SSLCertificateFile    /root/certificates/cert-server.pem
SSLCertificateKeyFile /root/certificates/key-server.pem

...

SSLCertificateChainFile /root/certificates/Terena-chain.pem
```

5) Modificare il file **/etc/apache2/ports.conf** come segue (per impedire l'ascolto della porta 80):

```
#NameVirtualHost *:80
#Listen 80
```

6) Assegnare i giusti permessi alla cartella dei file di LOG di SimpleSAMLphp:

```
chown www-data /opt/simplesamlphp/log
```

7) Modificare il file **/opt/simplesamlphp/config/config.php** come segue:

   a) Attivare la validazione dei metadati XML secondo gli schemi da loro indicati:

```
'debug.validatexml' => TRUE,
```

   b) Attivare la modalità di DEBUG per registrare tutti i messaggi che vengono scambiati durante la trasmissione da IDP a SP e viceversa:

```
'debug' => TRUE,
....
'logging.level'   => SimpleSAML_Logger::DEBUG,
'logging.handler' => 'file',
```

   (in questo modo i log verranno salvati nella cartella "**/opt/simplesamlphp/log/**" come stabilito dal file config.php)

   c) Impostare la password dell'amministratore della pagina di simpleSAMLphp (la si può generare con il comando `**php /opt/simplesamlphp/bin/pwgen.php**`):

```
'auth.adminpassword' => '{SSHA256}4c7N6k/2kHnY...LB0BxNA==',
```

   d) Generare una stringa casuale per il '**secretsalt**' con il comando:

```
tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32
count=1 2>/dev/null ; echo
```

   e inserirla nel 'secretsalt':

```
'secretsalt' => '869499p6ysve1iezf86h09zd6iwjuwz8',
```

   e) Completare con le informazioni riguardanti il Contatto Tecnico responsabile dell'IdP:

```
'technicalcontact_name' => 'Technical Contact',
'technicalcontact_email' => 'system.support@email.com',
```

   f) Settare la giusta Timezone:

```
'timezone' => 'Europe/Rome',
```

   g) Impostare la propria lingua di default:

```
'language.default' => 'it',
```

   h) Commentare tutto il contenuto dell' "**authproc.sp**"

8) Attivare il modulo SSL, Riavviare Apache2:

   - `cd /etc/apache2/mods-available/`
   - `a2enmod ssl`
   - `cd /etc/apache2/sites-available/`
   - `a2ensite default-ssl`
   - `service apache2 restart`

9) Provare ad accedere a **`https://ssp-sp.domain.it/simplesaml`**

7 Installare e Configurare il SimpleSAMLphp Service Provider

1) Creare un Certificato self-signed, valido 30 anni, con OpenSSL (SimpleSAMLphp non supporta con i certificati DSA, ma solo quelli RSA):
   - `cd /opt/simplesamlphp/cert`
   - `openssl req -newkey rsa:2048 -new -x509 -days 10950 -nodes -out server.crt -keyout server.pem`
2) Configurare SimpleSAMLphp per prelevare i Metadati della Federazione IDEM a intervalli regolari:
   a) Abilitare il modulo CRON per l'esecuzione del download dei Metadati di IDEM a intervalli regolari:
      - `cd /opt/simplesamlphp/`
      - `touch modules/cron/enable`
      - `cp modules/cron/config-templates/*.php config/`
   b) Abilitare il modulo METAREFRESH per il download ed il parsing corretto dei Metadati di IDEM:
      - `cd /opt/simplesamlphp/`
      - `touch modules/metarefresh/enable`
      - `cp modules/metarefresh/config-templates/*.php config/`
   c) Testare il corretto funzionamento del METAREFRESH:
      - `cd /opt/simplesamlphp/modules/metarefresh/bin`
      - `./metarefresh.php -s http://www.garr.it/idem-metadata/idem-test-metadata-sha256.xml > metarefresh-test.txt`

      Se l'output uscente produce errori contattare IDEM: idem-help@garr.it
   d) Modificare il file di configurazione del modulo CRON **vim /opt/simplesamlphp/config/module_cron.php** come segue:

```
$config = array (
/* Il valoreCASUALEsegreto
 * può essere generato con lo stesso comando usato
 * per il secretsalt
 */
   'key' => 'valoreCASUALEsegreto',
   'allowed_tags' => array('daily', 'hourly', 'frequent'),
   'debug_message' => FALSE,
   'sendemail' => FALSE,
);
```

e) Accedere alla pagina:

`https://ssp-sp.domain.it/simplesaml/module.php/cron/croninfo.php`

inserendo la password di Amministratore di SimpleSAMLphp.

f) Copiare l'esempio di file crontab che compare a video e incollarlo nel proprio con:

`crontab -e`

modificando l'ultima riga in:

```
# Esegui cron: [frequent]
*/30 * * * * curl --silent "https://ssp-sp.do-
main.it/simplesaml/module.php/cron/cron.php?key=valoreCASUALEsegreto&tag=frequent" >
/dev/null 2>&1
```

g) Modificare il file di configurazione del modulo METAREFRESH vim **/opt/simplesamlphp/config/config-metarefresh.php** come evidenziato:

```
   $config = array(
     'sets' => array(
       'idem' => array(
         'cron'      => array('hourly'),
         'sources'   => array(
            array(
              'src' => 'http://www.garr.it/idem-metadata/idem-test-metadata-
sha256.xml',
              'validateFingerprint' =>
'2F:F8:24:78:6A:A9:2D:91:29:19:2F:7B:33:33:FF:59:45:C1:7C:C8',
              'template' => array(
              'tags'  => array('idem'),
              'authproc' => array(
                51 => array(
                  'class' => 'core:AttributeMap', 'oid2name'),
                ),
              ),
            ),
         ),
         'expireAfter' => 60*60*24*5,  // Maximum 5 days cache time.
          // Il seguente PATH è punta a /opt/simplesamlphp
          'outputDir' => 'metadata/idem-federation/',
          /*
           * Which output format the metadata should be saved as.
           * Can be 'flatfile' or 'serialize'.
           * 'flatfile' is the default.
           */
          'outputFormat' => 'flatfile',
       ),
     ),
   );
```

h) Creare e assegnare i giusti permessi per permettere la creazione di file nella directory **/opt/simplesamlphp/metadata/idem-federation**:

- `mkdir /opt/simplesamlphp/metadata/idem-federation`
- `chown www-data /opt/simplesamlphp/metadata/idem-federation`

i) Modificare il file **/opt/simplesamlphp/config/config.php** nel seguente modo per indicare di utilizzare il nuovo file di metadata:

```
  'metadata.sources' => array(
    array('type' => 'flatfile'),
    array(
      'type' => 'flatfile',
      'directory' => 'metadata/idem-federation'
    ),
  ),
```

j) Rimuovere/Rinominare i file:
1. /opt/simplesamlphp/metadata/saml20-idp-remote.php
2. /opt/simplesamlphp/metadata/saml20-idp-hosted.php
3. /opt/simplesamlphp/metadata/saml20-sp-remote.php
4. /opt/simplesamlphp/metadata/shib13-idp-remote.php
5. /opt/simplesamlphp/metadata/shib13-idp-hosted.php
6. /opt/simplesamlphp/metadata/shib13-sp-hosted.php
7. /opt/simplesamlphp/metadata/shib13-sp-remote.php
8. /opt/simplesamlphp/metadata/wsfed-idp-remote.php
9. /opt/simplesamlphp/metadata/wsfed-sp-hosted.php

k) Forzare il download dei metadati accedendo alla scheda "**Federazione**" dal sito SimpleSAMLphp: **https://ssp-sp.domain.it/simplesaml/** e cliccando su "**Metarefresh: fetch metadata**" o attendere 1 giorno.

Modificare il valore di "**memory_limit**" in **/etc/php5/apache2/php.ini** ad almeno "**256M**" o più se non si è in grado di portare a termine il download e la trasformazione dei metadati.

3) Modificare il file **/opt/simplesamlphp/config/authsources.php** come segue (modificando opportunamente le parti evidenziate):

```
// An authentication source which can authenticate against both SAML 2.0
// and Shibboleth 1.3 IdPs.
// Into this example the Authentication Source is "example-sp"

'example-sp' => array(

  'saml:SP',


  // The entity ID of this SP.
  // Can be NULL/unset, in which case an entity ID
  // is generated based on the metadata URL

  'entityID' => NULL,


  // The entity ID of the IdP this should SP should contact.
```

```
// Can be NULL/unset,
// in which case the user will be shown a list of available IdPs.
'idp' => NULL,


// The URL to the discovery service.
// Can be NULL/unset,
// in which case a builtin discovery service will be used.
'discoURL' => NULL,


// Questo parametri punta a /opt/simplesamlphp/cert.
// La chiave e il certificato devono essere in formato PEM.
'privatekey' => 'server.pem',
'certificate' => 'server.crt',
'authproc' => array(
   // Questo filtro serve per convertire gli OID
   // in Nomi comprensibili all'uomo
   90 => array('class' => 'core:AttributeMap','oid2name'),
),

'UIInfo' => array(
  'DisplayName' => array(
    'en' => 'English SP Display Name',
    'it' => 'SP Display Name in Italiano',
  ),
  'Description' => array(
    'en' => 'Service Description',
    'it' => 'Descrizione del Servizio offerto',
  ),
  'PrivacyStatementURL' => array(
    'en' => 'https://www.your.organization.it/en/privacy',
    'it' => 'https://www.your.organization.it/it/privacy',
  ),
  'Logo' => array(
     array(
      'url'    => 'https://www.your.organization.it/en/logo80x60.png',
      'height' => 60,
      'width'  => 80,
     ),
     array(
      'url'    => 'https://www.your.organization.it/logo16x16.png',
      'height' => 16,
      'width'  => 16,
     ),
  ),


//name is required for AttributeConsumingService element.
'name' => array(
   'en' => 'Example Service Provider',
   'it' => 'Service Provider di esempio',
),
```

```
  'description' => array(
     'en' => 'Service Description',
     'it' => 'Descrizione del Servizio offerto',
  ),


  'OrganizationName' => array(
    'en' => 'Your Organization Name',
    'it' => 'Il nome della tua organizzazione',
  ),

  'OrganizationDisplayName' => array(
    'en' => 'Your Organization Display Name',
    'it' => 'Il Display Name della tua Organizzazione',
  ),


  'OrganizationURL' => array(
    'en' => 'https://www.your.organization.it/en',
    'it' => 'https://www.your.organization.it/it',
  ),


   'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',


   // Esempio di attributi utente richiesti NON OBBLIGATORIAMENTE
   // per la fruizione del servizio ospitato dall'SP.
   // Qui vi devono essere inseriti anche gli attributi che poi saranno OBBLIGATORI.
   // cn                        => urn:oid:2.5.4.3
   // mail                      => urn:oid:0.9.2342.19200300.100.1.3
   // eduPersonTargetedID       => urn:oid:1.3.6.1.4.1.5923.1.1.1.10
   // eduPersonPrincipalName    => urn:oid:1.3.6.1.4.1.5923.1.1.1.6
   'attributes' => array(
      'urn:oid:1.3.6.1.4.1.5923.1.1.1.10',
      'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',
      'urn:oid:0.9.2342.19200300.100.1.3',
      'urn:oid:2.5.4.3',
   ),
   // Esempio di attributi utente richiesti OBBLIGATORIAMENTE
   // per la fruizione del servizio ospitato dall'SP
   // cn                        => urn:oid:2.5.4.3
   // mail                      => urn:oid:0.9.2342.19200300.100.1.3
   // eduPersonTargetedID       => urn:oid:1.3.6.1.4.1.5923.1.1.1.10
   // eduPersonPrincipalName    => urn:oid:1.3.6.1.4.1.5923.1.1.1.6
   'attributes.required' => array(
      'urn:oid:1.3.6.1.4.1.5923.1.1.1.10',
      'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',
   ),
),
```

4) Modificare il file "**/opt/simplesamlphp/vendor/simplesamlphp/saml2/src/SAML2/XML/md/EntityDescriptor.php**" come segue per avere l'encoding ottimale sui metadati generati:

```
$doc = new DOMDocument('1.0','utf-8');
```

5) Registrare i propri Metadati, raggiungibili alla URL:
https://ssp-sp.domain.it/simplesaml/module.php/core/frontpage_federation.php premendo su "Mostra Metadati" del vostro SSP SP, sull' IDEM Entity Registry: https://registry.idem.garr.it

6) In caso di problemi contattare l'idem-help@garr.it

8 Applicazione di Test

Presupponendo che stiate utilizzando come DocumentRoot la cartella "**/var/www**", le seguenti operazioni vi porteranno ad ottenere un'applicazione di test che mostrerà gli attributi rilasciati dagli IdP:

1) Create il file "**index.php**" nella directory "**/var/www**" con il contenuto seguente:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

<html>

   <head>
      <title>SSP-SP Example Page</title>
   </head>

   <body>
      <p>This is an Example Page
         that show the behaviour of a SimpleSAMLphp Service Provider</p>

      <?php
         require_once('/opt/simplesamlphp/lib/_autoload.php');
         $as = new SimpleSAML_Auth_Simple('example-sp');
         $as->requireAuth();
         $attributes = $as->getAttributes();
         header('Content-Type: text/plain; charset=utf-8');
7)       foreach ($attributes as $name => $values) {
            echo("$name:\n");
            foreach ($values as $value) {
               echo("\t$value\n");
            }
            echo("\n");
         }
      ?>
   </body>

</html>
```

2) Riavviate Apache2: `service apache2 restart`

3) Provare ad accedere alla pagina **https://ssp-sp.domain.it/index.php**

9 Approfondimenti

9.1 Discojuice Discovery Service Embedded

1. Creare una cartella "**DS**" nella propria DocumentRoot (es.: **/var/www/DS**)

2. Inserirvi la "**discojuiceDiscoveryResponse.html**":
   - `cd /var/www/DS`
   - `wget https://raw.github.com/andreassolberg/DiscoJuice/master/discojuice/discojuiceDiscoveryResponse.html`

3. Creare la pagina **/var/www/disco.html** contenente:

```
<html>
<head>
    <meta charset="utf-8" />
    <title>Select your IDP</title>

    <link rel="shortcut icon"
href="http://discojuice.bridge.uninett.no/simplesaml/module.php/discojuice/favi-
con.png" />

    <!-- JQuery hosted by Google -->
    <script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"
type="text/javascript"></script>

    <!-- DiscoJuice hosted by UNINETT at discojuice.org -->
    <script type="text/javascript" src="https://cdn.discojuice.org/engine/disco-
juice-stable.min.js"></script>
    <link rel="stylesheet" type="text/css" href="https://cdn.discojuice.org/css/di-
scojuice.css" />
    <script type="text/javascript">
       $(document).ready(function() {
          var target = "a.login-btn";
          var redirectUrl = $(target).attr('href');
          var popupTitle = "###NOME SP o ALTRO TITOLO PER IL POPUP - CHANGE ME###";
          var spEntityID = "###YOUR SSP-SP EntityID - CHANGE ME###";
          var authSource = "###YOUR-SP-AUTHSOURCE - CHANGE ME###";
          var spFQDN = "###YOUR.SP.FQDN - CHANGE ME###";
```

```
          DiscoJuice.Hosted.setup(
             {
              "target": target,
              "title": popupTitle,
              "spentityid": spEntityID,
              "responseurl": "https://"+ spFQDN +"/DS/discojuiceDiscoveryResponse.-
html",
              "redirectURL": "https://+spFQDN+/simplesaml/module.php/core/as_login.-
php?AuthId="+ authSource +"&ReturnTo="+ redirectUrl +"&saml:idp=",
              "feeds": ["garr-test"]
             }
          );
      });
   </script>
  </head>
<body style="background: #ccc">
   <p><a class="login-btn" href="/index.php">Login con IDEM</a></p>
</body>
</html>
```

4. Modificare **.../simplesamlphp/config/authsources.php** cambiando il valore di "**discoUrl**" in:

```
...
'discoURL' => 'https://###YOUR.FQDN.SP - CHANGE ME###/DS/disco.html',
...
```

5. Provare ad accedere alla "**index.php**".

9.2 Auth Mem Cookie: Usare Applicazioni non-PHP con SimpleSAMLphp

1. Installare i pacchetti necessari
   - `sudo apt-get install mysql-server php5-mysql php5-dev php5-memcache memcached libmemcached-tools php-pear build-essential apache2-prefork-dev` (configurando il DB di mySQL e rispondendo "**Yes**" alla domanda "`Enable memcache session handler support? [yes]:`")

2. Aggiungere memcached a memcache.ini:
   - `echo "extension=memcache.so" | sudo tee /etc/php5/conf.d/memcache.ini`

3. Verificare che memcached sia funzionante:
   - `ps aux | grep memcached`

4. Prelevare l'ultima versione del modulo Auth MemCache Cookie in **/opt/**:
   - `cd /opt ; wget http://sourceforge.net/projects/authmemcookie/files/latest/download -O /opt/mod_authmemcookie.tar.gz`

5. Estrarre il pacchetto scaricato:
   - `tar xzvf mod_authmemcookie.tar.gz`

6. Editare il file "**/opt/mod_authmemcookie/Makefile**" inserendo:

```
MY_APXS=/usr/bin/apxs2
MY_LDFLAGS=-lmemcache -L/mnt/distributions/rpmbuilds/ste-1.0/ste-php/TMP/SFR-
libmemcache-1.4.0.rc2-build/product/sfr-suse-addon/lib -L/usr/include
```

7. Installare il modulo Auth Mem Cookie:
   - `cd /opt/mod_authmemcookie ; make ; make install`

8. Editare il **/etc/apache2/site-enabled/default-ssl** in modo che contenga:

```
   <IfModule mod_auth_memcookie.c>
      <Directory />
        # This is a list of memcache servers which Auth MemCookie
        # should use. It is a ','-separated list of
        # host:port-pairs.
        # Note that this list must list the same servers as the
        # 'authmemcookie.servers'-option in config.php in the
        # configuration for SimpleSAMLphp.
        Auth_memCookie_Memcached_AddrPort "127.0.0.1:11211"

        # This must be set to 'on' to enable Auth MemCookie for
        # this directory.
        Auth_memCookie_Authoritative on

        # This adjusts the maximum number of data elements in the
        # session data. The default is 10, which can be to low.
        Auth_memCookie_SessionTableSize "40"

        # These two commands are required to enable access control
        # in Apache.
        AuthType Cookie
        AuthName "My Login"
```

```
      # This command causes apache to redirect to the given
      # URL when we receive a '401 Authorization Required'
      # error. We redirect to "/simplesaml/authmemcookie.php",
      # which initializes a login to the IdP.
      ErrorDocument 401 "/simplesaml/authmemcookie.php"
    </Directory>
  </IfModule>

    <Location /secret>
      # This allows all authenticated users to access the
      # directory. To learn more about the 'Require' command,
      # please look at:
      # http://httpd.apache.org/docs/2.0/mod/core.html#require
      Require valid-user
    </Location>
```

9. Modificare il file "**config/authmemcookie.php**" inserendo il proprio authsource. (Ex.: **example-sp**):

```
...
'authsource' => 'example-sp',
...
'username' => 'uid',
```

10. Edita il **/opt/simplesamlphp/config/config.php** per abilitare il modulo Auth MemCookie:

```
'enable.authmemcookie' => true,
```

11. Abilita il nuovo modulo in Apache2:
    - `vim /etc/apache2/mods-available/mod_auth_memcookie.load` :

```
LoadModule mod_auth_memcookie_module /usr/lib/apache2/modules/mod_auth_memcookie.so
```

    - `a2enmod mod_auth_memcookie`

12. Create la vostra applicazione di test che stampi le variabili di sessione che riceve dagli IdP:
    - `mkdir /var/www/secret ; vim /var/www/secret/index.php:`

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>

<head>
  <title>SSP-SP Example Page</title>
</head>

<body>

<p>This is an Example Page that show the behaviour of a SimpleSAMLphp Service
Provider</p>

<table>
   <?php
```

```
      foreach($_SERVER as $key=>$value) {
         echo('<tr><td>' . htmlspecialchars($key) . '</td><td>' .
htmlspecialchars($value) . '</td></tr>');
      }
   ?>
</table>
</body>
</html>
```

13. Riavviate Apache2:
    - `service apache2 restart`

14. Provate ad accedere alla pagina **https://ssp-sp.domain.it/secret**

9.3 Aggiornare SimpleSAMLphp alla versione successiva

1. Prelevare la nuova versione di SimpleSAMLphp ed estrarla nella directory **/opt:**
   - `cd /opt ; wget https://simplesamlphp.org/res/downloads/simplesamlphp-XX.YY.ZZ.tar.gz ; tar xzvf simplesamlphp-XX.YY.ZZ.tar.gz`

     (verificare cosa è necessario avere dal sito di SimpleSAMLphp)

2. Rimuovere le cartelle "**config**" e "**metadata**" presenti nella nuova versione:
   - `cd /opt/simplesamlphp-XX.YY.ZZ/ ; rm -rf config metadata`

3. Copiare i vecchi file di configurazione dalla vecchia versione alla nuova:
   - `cd /opt/simplesamlphp-XX.YY.ZZ`
   - `cp -rv /opt/simplesamlphp/config config`
   - `cp -rv /opt/simplesamlphp/metadata metadata`

4. Copiare il certificato e la chiave dalla versione precedente a quella nuova:
   - `cp -Rf /opt/simplesamlphp/cert /opt/simplesamlphp-XX.YY.ZZ/`

5. Controllare se sono state apportate differenze al nuovo **config.php**:
   - `diff /opt/simplesamlphp/config-templates/config.php /opt/simplesamlphp-1.12.0/config-templates/config.php`

6. Sostituire la vecchia versione con la nuova:
   - `cd /opt`
   - `mv simplesamlphp simplesamlphp-OLD`
   - `mv simplesamlphp-XX.YY.ZZ simplesamlphp`

7. Permettere ad Apache2 di scrivere sul file di LOG di SimpleSAMLphp e sui metadati:
   - `chown www-data /opt/simplesamlphp/log`
   - `chown www-data /opt/simplesamlphp/metadata/idem-federation`

8. Copiare/Abilitare i moduli aggiuntivi inseriti nella vecchia versione:
   - `cd /opt/simplesamlphp`
   - `cp -rf /opt/simplesamlphp-OLD/simplesaml-attributepolicy .`
   - `cd /opt/simplesamlphp/modules`
   - `ln -s /opt/simplesamlphp/simplesaml-attributepolicy/attributepolicy/`
   - `touch cron/enable`
   - `touch metarefresh/enable`

9. Modificare il file "**/opt/simplesamlphp/vendor/simplesamlphp/saml2/src/SAML2/XML/md/EntityDescriptor.php**" come segue per avere un encoding ottimale sui metadati generati:

```
$doc = new DOMDocument('1.0','utf-8');
```