Installazione SimpleSAMLphp Identity Provider su Debian-Linux
+
Upgrade

28 Gennaio 2015

Autore: Marco Malavolti

Indice generale

1) Introduzione....3
2) Software da installare....3
3) Richiedere il certificato HTTPS per l'SP....4
4) Modifica del file hosts....4
5) Installare i pacchetti necessari....4
6) Installare SimpleSAMLphp v1.13.2....5
7) Installare e Configurare il SimpleSAMLphp Identity Provider....7
8) Approfondimenti....15
8.1) Esempio di "module_attributepolicy.php"....15
8.2) Aggiornare SimpleSAMLphp alla versione successiva....16

1 Introduzione

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

2 Software da installare

- openssl
- ntp
- nmap
- apache2
- curl
- cron
- git
- php5 (>=5.3)
- php5-mcrypt
- php5-ldap
- 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 docu- mentazione 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 l'Identity Provider di SimpleSAMLphp:

```
127.0.1.1 ssp-idp.domain.it ssp-idp
```

5 Installare i pacchetti necessari

a) `sudo apt-get install apache2 openssl ntp nmap vim php5 php5-mcrypt php5-ldap curl git cron`

b) Aprire le seguenti porte sul/sui firewall:

1) 443 => HTTPS (da e verso la rete internet)
2) 389 => LDAP (da e verso il server LDAP)
3) 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-idp.domain.it** o da **http://127.0.1.1**.

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:
   - `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 "**authproc.idp**" e il "**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-idp.domain.it/simplesaml`**

7 Installare e Configurare il SimpleSAMLphp Identity Provider

1) Creare un Certificato self-signed, valido 30 anni, con OpenSSL (SimpleSAMLphp non supporta con i certificati DSA, ma solo quelli RSA):
   - `mkdir /opt/simplesamlphp/cert ; 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`
   d) Se l'output uscente produce errori contattare IDEM: idem-help@garr.it
   e) 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' => TRUE,
   'sendemail' => FALSE,
);
```

f) Accedere alla pagina come Amministratore di SimpleSAMLphp:

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

g) 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-idp.domain.it/simplesaml/modu-
le.php/cron/cron.php?key=valoreCASUALEsegreto&tag=frequent" > /dev/null
2>&1
```

h) 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-meta-
data-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 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',
      ),
     ),
  );
```

i) Creare la cartella che conterrà i metadati e assegnarle i giusti permessi:
   - `mkdir /opt/simplesamlphp/metadata/idem-federation`
   - `chown www-data /opt/simplesamlphp/metadata/idem-federation`

j) 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'
   ),
  ),
```

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

l) Forzare il download dei metadati accedendo alla scheda "**Federazione**" dal sito SimpleSAMLphp: **https://ssp-idp.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) Attivare il modulo per il Consenso Informato:
   - `touch /opt/simplesamlphp/modules/consent/enable`

4) Modificare il file **/opt/simplesamlphp/config/config.php** per abilitare il supporto SAML2.0 e SAML 1.x:

```
'enable.saml20-idp' => true,
// Settare a false per disabilitare il supporto SAML v1.x
'enable.shib13-idp' => true,
```

5) Modificare il file **/opt/simplesamlphp/config/authsources.php** per configurare l'Authentication Module LDAP:

   a) Rimuovere il commento al Frammento di codice che comincia con "// **Example of a LDAP authentication source.**"

   b) Rinominare la voce "**example-ldap**" con un valore più significativo per il proprio LDAP (Es.: **org-ldap**)

   c) Inserire le informazioni richieste per il corretto collegamento con il proprio LDAP:

```
// Es.: 'ldaps://ldap1.domain.it ldaps://ldap2.domain.it' raggiungibili
'hostname' => 'ldap.domain.it',

// Impostare a FALSE se non avete impostato il TLS sul vostro LDAP
'enable_tls' => TRUE,


// Non modificare il valore dello uid se non necessario
'dnpattern' => 'uid=%username%,ou=people,dc=example,dc=org',
```

   d) Configurare i metadati dell'IdP editando il file **/opt/simplesamlphp/metadata/saml20-idp-hosted.php** e il file **/opt/simplesamlphp/metadata/shib13-idp-hosted.php**:

```
$metadata['__DYNAMIC:1__'] = array(
   'host' => '__DEFAULT__',


   /* X.509 key and certificate. Relative to the cert directory.
    * The Key MUST BE in PEM format
    */
   'privatekey' => 'server.pem',
   'certificate' => 'server.crt',


   /*
    * Authentication source to use. Must be one that is configured in
    * 'config/authsources.php'.
    */
    'auth' => 'org-ldap',
    'scope' => array('domain.it'),
    'userid.attribute' => 'uid',


    'UIInfo' => array(
       'DisplayName' => array(
          'en' => 'English IDP Display Name',
          'it' => 'IDP Display Name in Italiano',
        ),
       'Description' => array(
          'en' => 'Identity Provider for the users of University X',
          'it' => 'Identity Provider per gli utenti dell\' Università X',
       ),
       'InformationURL' => array(
```

```
         'en' => 'https://www.your.organization.it/en/info',
         'it' => 'https://www.your.organization.it/it/info',
      ),
      '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/logo80x60.png',
           'height' => 60,
           'width'  => 80,
         ),
         array(
           'url'    => 'https://www.your.organization.it/logo16x16.png',
           'height' => 16,
           'width'  => 16,
         ),
      ),
   ),
   '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',
   ),


   /*
    * Authentication processing filters that will be executed for this IdP
    * Both SAML 1.x and SAML 2.0
    */
    'authproc' => array(
      // Add schacHomeOrganization for domain of entity
      10 => array(
         'class' => 'core:AttributeAdd',
         'schacHomeOrganization' => 'domain.it',
         'schacHomeOrganizationType' =>
'urn:schac:homeOrganizationType:int:university',
      ),


      // Add eduPersonPrincipalName
      11 => array (
         'class' => 'core:ScopeAttribute',
         'scopeAttribute'  => 'schacHomeOrganization',
         'sourceAttribute' => 'uid',
         'targetAttribute' => 'eduPersonPrincipalName',
      ),
```

```
      //Add eduPersonScopedAffiliation
      12 => array(
         'class' => 'core:ScopeAttribute',
         'scopeAttribute'  => 'eduPersonPrincipalName',
         'sourceAttribute' => 'eduPersonAffiliation',
         'targetAttribute' => 'eduPersonScopedAffiliation',
      ),


      // Adopts language from attribute to use in UI
      30 => 'core:LanguageAdaptor',


      // Consent module is enabled(with no permanent storage, using cookies)
      97 => array(
         'class'  => 'consent:Consent',
         'store'  => 'consent:Cookie',
         'focus'  => 'yes',
         'checked'   => FALSE
      ),


      // Enable this authproc filter to automatically generated eduPersonTargetedID
      98 => array(
         'class' => 'core:TargetedID',
         'nameId' => TRUE,
         ),


      // If language is set in Consent module it will be added as an attribute
      99 => 'core:LanguageAdaptor',


      // Convert LDAP names to oids.
      100 => array('class' => 'core:AttributeMap', 'name2oid'),

   ),


   'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
   'attributeencodings' => array(
                              'urn:oid:1.3.6.1.4.1.5923.1.1.1.10' => 'raw',
                           ),
);
```

6) Completare i file **/opt/simplesamlphp/attributemap/name2oid.php** con gli OID mancanti per riconoscere i nuovi attributi:

   'schacHomeOrganizationType' => '1.3.6.1.4.1.25178.1.2.10',

7) Aggiungere la traduzione per lo schacHomeOrganizationType da mostrare nella pagina del Consenso Informato:
   a) Modificare il file **/opt/simplesamlphp/dictionaries/attributes.definition.json** inserendo in coda questo:

```
        ...
    "attribute_schachomeorganizationtype":{
        "en": "Home Organization Type"
    }
```

   b) Modificare il file **/opt/simplesamlphp/dictionaries/attributes.translation.json** inserendo in coda questo:

```
    "attribute_schachomeorganizationtype":{
        "it": "Tipo di Organizzazione"
    },
```

NOTA BENE: Anche una virgola di troppo fa fallire la traduzione, quindi, prestare molta attenzione.

8) Configurazione dell'Attribute Release Policy attraverso il modulo sviluppato da Riccardo Valzorio:
   a) Importare e attivare il modulo "**simplesaml-attributepolicy**" in SimpleSAMLphp:
      - `cd /opt/simplesamlphp/`
      - `git clone https://github.com/RikV/simplesaml-attributepolicy.git`
      - `cd /opt/simplesamlphp/modules`
      - `ln -s /opt/simplesamlphp/simplesaml-attributepolicy/attributepolicy/ .`
      - `touch /opt/simplesamlphp/modules/attributepolicy/enable`

   b) Copiare il template del file di configurazione del modulo:
      - `cd /opt/simplesamlphp/config`
      - `cp /opt/simplesamlphp/modules/attributepolicy/config-template/module_attributepolicy.php .`

   c) Prelevare il '*module_attributepolicy_test.php.txt*' della Federazione IDEM di Test, rinominarlo in '**module_attributepolicy.php**' e inserirlo in **/opt/simplesamlphp/config/:**

```
wget https://www.idem.garr.it/documenti/doc_download/355-module-attributepolicy-test-php -O module_attributepolicy.php
```

   d) Modificare i file **/opt/simplesamlphp/metadata/saml20-idp-hosted.php** e **/opt/simplesamlphp/metadata/shib13-idp-hosted.php** inserendo, sotto la voce "**authproc**", la linea seguente:

```
...
40 => 'attributepolicy:AttributePolicy',
```

```
    ...
```

e) Modificare la riga 195 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');
```

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

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

8 Approfondimenti

8.1 Esempio di "module_attributepolicy.php"

```
<?php


/*
 * AttributePolicy configuration file.
 *
 * Define the attributes to release:
 * - by default
 * - by EntityID
 * - by a regular expression based on EntityID
 *
 */
$config = array(

   // Default Attribute Policy that release ePTID and ePSA to all SP
   'default' => array('eduPersonTargetedID', 'eduPersonScopedAffiliation'),

   // Attribute Policy for shib-sp.example.com
   'https://shib-sp.example.com/shibboleth' => array(
      'givenName',
      'sn',
      'cn',
      'mail',
      'eduPersonPrincipalName',
      'eduPersonScopedAffiliation'
   ),

   // Attribute Policy for ssp-sp.example.com
   'https://ssp-
sp.example.com/simplesaml/module.php/saml/sp/metadata.php/ssp-sp' => array(
      'givenName',
      'sn',
      'mail',
      'telephoneNumber',
      'eduPersonPrincipalName',
   ),
);
```

8.2 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');
```