Desenvolvimento - Proxy IdP CAFé

Pré-requisitos:

Sistema Operacional: **Linux Debian 8**
SimpleSAMLPHP: **1.14.2**

Instalação

Para realizar a instalação dos componentes do Proxy IdP CAFé, siga os passos a seguir.

Instalação SimpleSAMLPHP

Instalação dos pacotes do servidor web e PHP:

```
# apt-get install php5 php5-cli php5-common php5-mcrypt libapache2-mod-php5 apache2 vim ngrep dnsutils tcpdump
```

Habilitar módulos do Apache2:

```
# a2enmod rewrite
# a2enmod ssl
# service apache2 restart
```

Descompactar pacote do SimpleSAMLPHP:

```
# cd /var
# wget --no-check-certificate https://simplesamlphp.org/res/downloads/simplesamlphp-1.14.2.tar.gz
# tar xzvf simplesamlphp-1.14.2.tar.gz
# ln -s simplesamlphp-1.14.2 simplesamlphp
```

Criação do Certificado para o Apache2

IMPORTANTE: Ao gerar o certificado, utilizar o nome FQDN da máquina (nome completo)

Para gerar o certificado, execute o seguinte comando, refletindo as configurações para o servidor instalado:

```
# openssl req $@ -new -x509 -days 3650 -nodes -out /etc/apache2/apache.pem -keyout /etc/apache2/apache.pem
Generating a 2048 bit RSA private key
.............................................+++
.....+++
writing new private key to '/etc/apache2/apache.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:RJ
Locality Name (eg, city) []:Rio de Janeiro
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RNP
Organizational Unit Name (eg, section) []:RJ
Common Name (e.g. server FQDN or YOUR name) []:monipe-idp-proxy.rnp.br
Email Address []:suporte@monipe.rnp.br
```

Alteração das permissões do certificado:

```
# chmod 600 /etc/apache2/apache.pem
```

Configuração do acesso do SimpleSAMLPHP no Apache2

Criar o arquivo **/etc/apache2/sites-available/simplesamlphp.conf** com o seguinte conteúdo:

```
<VirtualHost *:80>
        ServerAdmin suporte@monipe.rnp.br
        ServerSignature Off

        # Redirecionamento para SSL
        RewriteEngine on
        RewriteCond %{HTTPS} !=on
        RewriteRule ^(.*) https://%{SERVER_NAME} [R,L]
</VirtualHost>

<VirtualHost *:443>
        ServerSignature Off
        SSLEngine on
        SSLCertificateFile /etc/apache2/apache.pem

        DocumentRoot /var/simplesamlphp/www
        Alias /simplesaml /var/simplesamlphp/www

        SSLProtocol All -SSLv2 -SSLv3

        <Location /simplesaml>
                Require all granted
        </Location>
</VirtualHost>
```

Habilitar o SimpleSAML no Apache2:

```
# a2ensite simplesamlphp
# service apache2 reload
```

Configuração das credenciais do SimpleSAMLPHP

Gerar a senha para o SimpleSAMLPHP. Guardar a senha gerada para realizar a configuração do SimpleSAMLPHP:

```
# /var/simplesamlphp/bin/pwgen.php
Enter password: mon2rnp
The following hashing algorithms are available:
md2          md4          md5          sha1         sha224       sha256
sha384       sha512       ripemd128    ripemd160    ripemd256    ripemd320
whirlpool    tiger128,3   tiger160,3   tiger192,3   tiger128,4   tiger160,4
tiger192,4   snefru       snefru256    gost         adler32      crc32
crc32b       fnv132       fnv164       joaat        haval128,3   haval160,3
haval192,3   haval224,3   haval256,3   haval128,4   haval160,4   haval192,4
haval224,4   haval256,4   haval128,5   haval160,5   haval192,5   haval224,5
haval256,5

Which one do you want? [sha256]
Do you want to use a salt? (yes/no) [yes] yes

  {SSHA256}irxvSGvbykKqNd/4knTr7wW/SWH+/QaTUjDhVhsNqork87Ou++Bakg==
```

Gerar um salto para a senha. Guardar o salto gerado para realizar a configuração do SimpleSAMLPHP:

```
# tr -c -d '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVXYZ#$!@%&*+-' </dev/urandom | dd bs=32
count=1 2>/dev/null;echo
iLq!hbIo9&@3O-glv1MR*n80bPcVmxAt
```

Configurar o SimpleSAMLPHP, editando o arquivo /var/simplesamlphp/config/config.php, alterando as variáveis abaixo. Para a variável auth.
adminpassword utilize a saída da senha gerada acima e para a variável secretsalt utilize o salto gerado acima. Demais variáveis, utilizar o indicado abaixo:

```
'auth.adminpassword'        => '{SSHA256}irxvSGvbykKqNd/4knTr7wW/SWH+/QaTUjDhVhsNqork87Ou++Bakg==,
'secretsalt' => 'iLq!hbIo9&@3O-glv1MR*n80bPcVmxAt',

'technicalcontact_name'     => 'MonIPE',
'technicalcontact_email'    => 'suporte@monipe.rnp.br',

'language.default'      => 'no',
'timezone' => 'America/Sao_Paulo',
```

Criação da chave para o SimpleSAMLPHP

IMPORTANTE: Ao gerar o certificado, utilizar o nome FQDN da máquina (nome completo)

Geração do certificado para o SimpleSAMLPHP:

```
# cd /var/simplesamlphp/cert
# openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out spssp.crt -keyout spssp.pem
Generating a 2048 bit RSA private key
..............+++
...+++
writing new private key to 'spssp.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:RJ
Locality Name (eg, city) []:Rio de Janeiro
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RNP
Organizational Unit Name (eg, section) []:RJ
Common Name (e.g. server FQDN or YOUR name) []:monipe-idp-proxy.rnp.br
Email Address []:suporte@monipe.rnp.br
```

Editar o arquivo /var/simplesamlphp/config/authsources.php para configurar as autoridades certificadoras, alterando o índice do array de 'default-sp' para 'monipe-sp':

```
    'monipe-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,

        'privatekey' => 'spssp.pem',

        'certificate' => 'spssp.crt',
```

Configuração do SimpleSAMLPHP

Para habilitar o envio de e-mails pelo SimpleSAMLPHP, executar o seguinte comandos:

```
# cd /var/simplesamlphp/modules/consent
# touch enable
```

Para configurar o SimpleSAMLPHP para atuar como SP e IdP, deve-se ajustar a configuração do arquivo /var/simplesamlphp/metadata/saml20-idp-hosted.php como exemplificado abaixo:

```
    'auth' => 'monipe-sp',
    'privatekey' => 'spssp.pem',
    'certificate' => 'spssp.crt',

    'auth' => 'monipe-sp',

    'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
    'authproc' => array(
        // Convert LDAP names to oids.
        100 => array('class' => 'core:AttributeMap', 'name2oid'),
    ),

    'UIInfo' => array(
        'DisplayName' => array(
            'en' => 'IdP MonIPE Proxy',
         ),
        'Logo' => array(
            array(
                'url'    => 'https://[URI_DNS_NAME]/simplesaml/module.php/monipe/img/monipe.png',
                'height' => 51,
                'width'  => 107,
            ),
         ),
     ),
```

Realizar a configuração do arquivo **/var/simplesamlphp/config/config.php** para habilitar a função de IdP e realizar mapeamento de atributos entre o SimpleSAMLPHP e CAFé:

```
...
    'enable.saml20-idp' => true,
...
    'authproc.idp' => array(
        // Adopts language from attribute to use in UI
        30 => 'core:LanguageAdaptor',
        // If language is set in Consent module it will be added as an attribute.
        99 => 'core:LanguageAdaptor',
        10 => array(
            'class' => 'core:AttributeMap', 'name2oid'
        ),
        20 => 'core:TargetedID',
        40 => 'core:AttributeRealm',
        50 => 'core:AttributeLimit',
    ),
    'authproc.sp' => array(
        50 => array(
            'class' => 'core:AttributeMap','oid2name',),
        // Adopts language from attribute to use in UI
        90 => 'core:LanguageAdaptor',
    ),
```

Para verificar que o SimpleSAMLPHP está corretamente configurado, acessar o endereço do Proxy via navegador utilizando o FQDN no endereço (Ex: **https://monipe-idp-proxy.rnp.br/simplesaml/**). Entrar na aba **Configuração**, deve apresentar uma tela semelhante da figura abaixo, destacando que o **SAML 2.0 IdP** está funcionando:

Tela de configurações do SimplePHPSAML

Publicação do metadata na CAFé

Para publicar o metadata na CAFé, executar os seguintes passos:

1. Entrar no Proxy via navegador utilizando o FQDN no endereço (Ex: **https://monipe-idp-proxy.rnp.br/simplesaml/**);
2. Entrar na aba **Federação** e clicar em **Mostrar Metadata** da seção **SAML 2.0 SP Metadata**;
3. Copiar conteúdo do Metadata **Em formato SAML 2.0 Metadata XML** e gerar um arquivo XML externo com o conteúdo copiado e;
4. Enviar via e-mail o **arquivo XML** gerado para a CAFé para que o **Proxy IdP CAFé** seja adicionado como host confiável.

Listagem de IdPs da CAFé

Para preencher a listagem de IdPs da CAFé no Proxy, siga os seguintes passos:

1. Baixar o arquivo: https://ds.cafeexpresso.rnp.br/metadata/ds-metadata.xml **(AJUSTAR PARA O ENDEREÇO DA CAFé)**
2. Entrar no Proxy via navegador utilizando o FQDN no endereço (Ex: **https://monipe-idp-proxy.rnp.br/simplesaml/**) e clicar na aba **Federação**, link **Conversor de XML para metadata do simpleSAMLphp**;
3. Colar o conteúdo do arquivo **ds-metadata.xml** recém baixado no campo de **Parser** e clicar no botão **Parse** e;
4. Colar a Metadata convertida do campo **saml20-idp-remote** no arquivo **/var/simplesamlphp/metadata/saml20-idp-remote.php** preservando a inicialização do PHP.

Teste de Autenticação com a CAFé

Para testar a autenticação com a CAFé, executar os seguintes passos:

1. Entrar no Proxy via navegador utilizando o FQDN no endereço (Ex: **https://monipe-idp-proxy.rnp.br/simplesaml/**);
2. Entrar na aba **Autenticação** e clicar no link **Test konfigurerte autentiseringskilder**;
3. Clicar no link **monipe-sp** e;
4. Selecionar um SP e tentar autenticação com um usuário da CAFé válido.

Inserção de Portais no Proxy

Para adicionar os portais no Proxy, é necessário adicionar novas entradas no array **medadata** no arquivo **/var/simplesamlphp/metadata/saml20-sp-remote.php**, como exemplificado abaixo, substituindo o endereços **monipe-portal-instituicao.rnp.br** pelo endereço FQDN do portal a ser inserido no Proxy:

```
$metadata['https://monipe-portal-instituicao.rnp.br/shibboleth-sp2'] = array(
    'name' => array(
        'pt_br' => 'Portal Institucional',
        'en' => 'Institution Portal',
    ),
    'AssertionConsumerService' => 'https://monipe-portal-instituicao.rnp.br/Shibboleth.sso/SAML/POST',
    'base64attributes'         => FALSE,
    'AssertionConsumerService' => array (
        0 => array (
            'index' => 0,
            'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
            'Location' => 'https://monipe-portal-instituicao.rnp.br/Shibboleth.sso/SAML2/POST',
        ),
    )
);
```