SAML Single Sign-On avec Pandora FMS

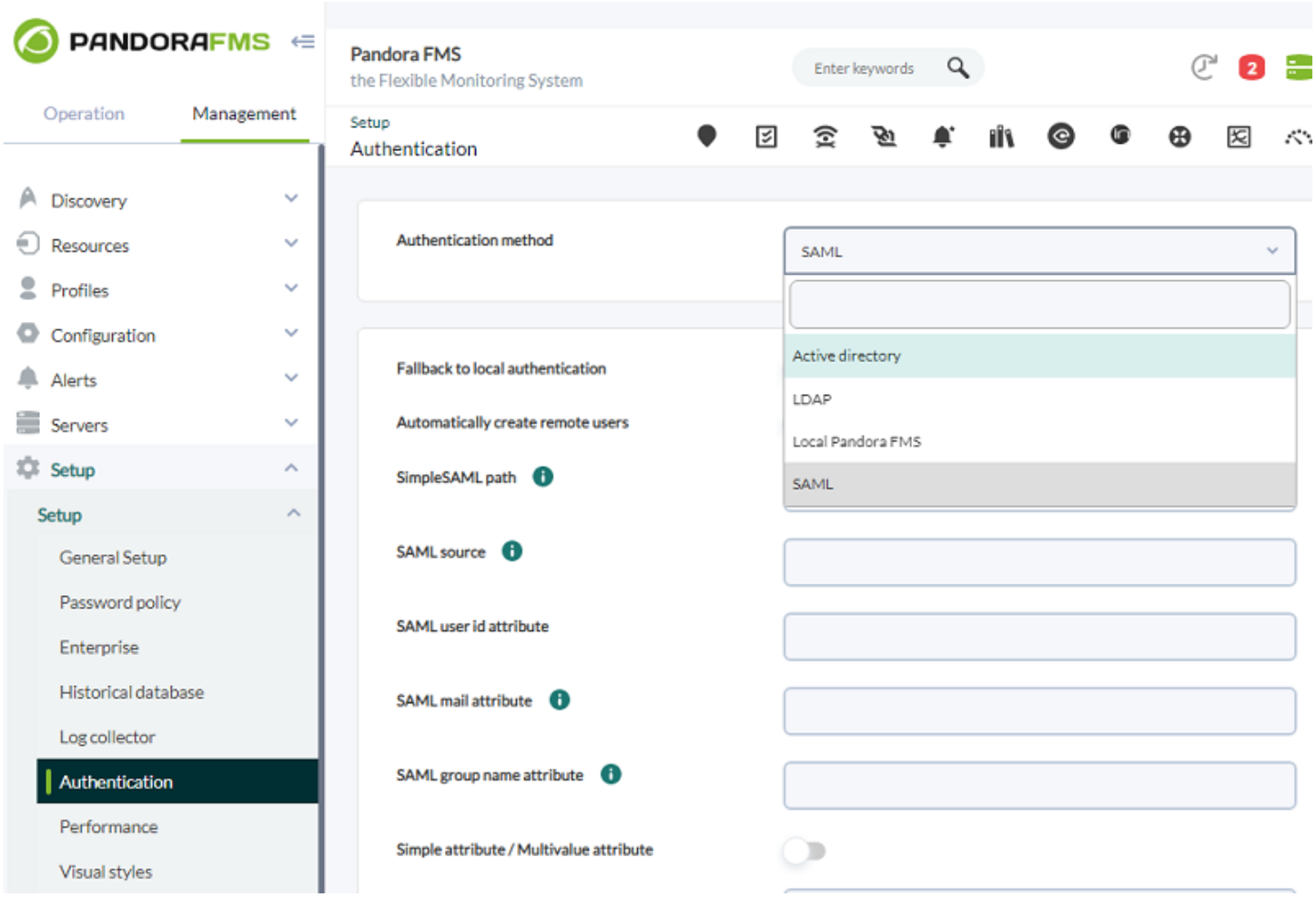
SAML Single Sign-On avec Pandora FMS

SAML est une norme ouverte d'authentification et d'autorisation basée sur XML. Pandora FMS peut fonctionner comme un fournisseur de services avec votre fournisseur d'identité SAML interne.

Les administrateurs s'authentifient toujours par rapport à la base de données locale.

Configurant Pandora FMS

Il faudra se rendre à Management → Setup → Setup → Authentication et sélectionnez SAML sous Authentication method.



Configuration du fournisseur de services

Pour configurer le fournisseur de services, téléchargez les éléments suivants SimpleSamlphp et installez-les dans `/opt/simplesamlphp/`.

Un *endpoint* devra être configuré pour gérer les authentifications en `/simplesaml` :

```
ln -s /opt/simplesamlphp/www /var/www/html/simplesaml
```

Vous devrez ajouter votre SP dans `/opt/simplesamlphp/config/authsources.php` :

```
'test-sp' => [
       'saml:SP',
       'entityID' => 'http://app.example.com',
       'idp' => 'http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php',
   ],
```

Les métadonnées du `idP` :

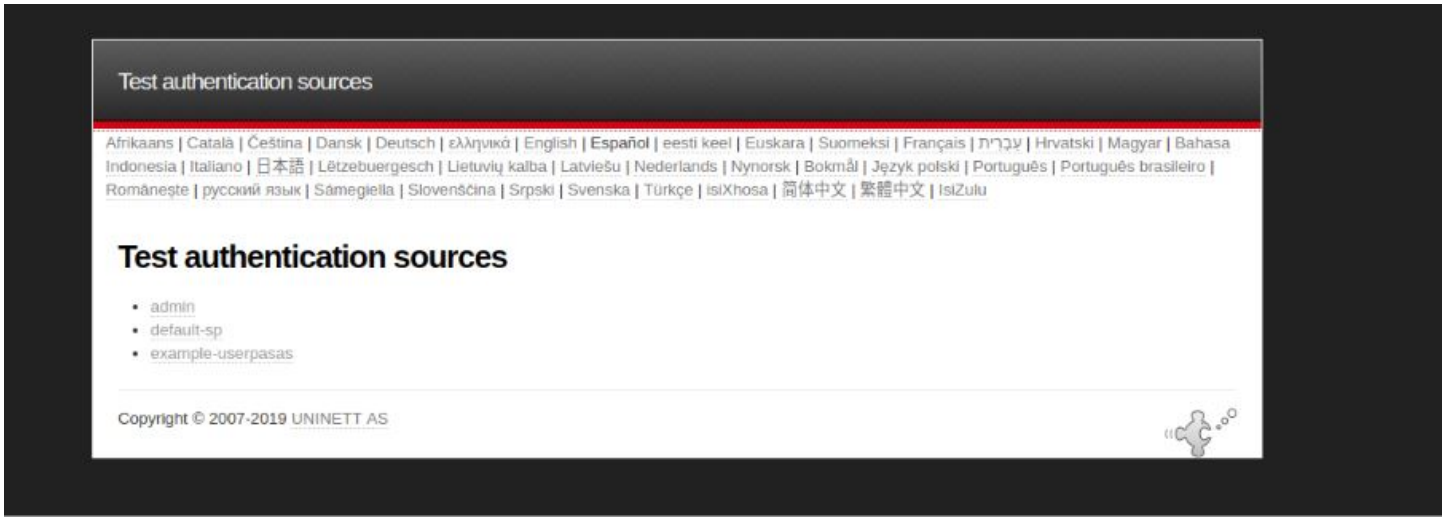
```
$metadata['http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php'] = array(
       'name' => array(
           'en' => 'Test IdP',
       ),
       'description' => 'Test IdP',
       'SingleSignOnService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SSOService.php',
       'SingleLogoutService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SingleLogoutService.php',
       'certFingerprint' => '119b9e027959cdb7c662cfd075d9e2ef384e445f',
   );
```

Il est recommandé d'utiliser la validation du certificat avec un certificat direct au lieu de `certFingerprint`.

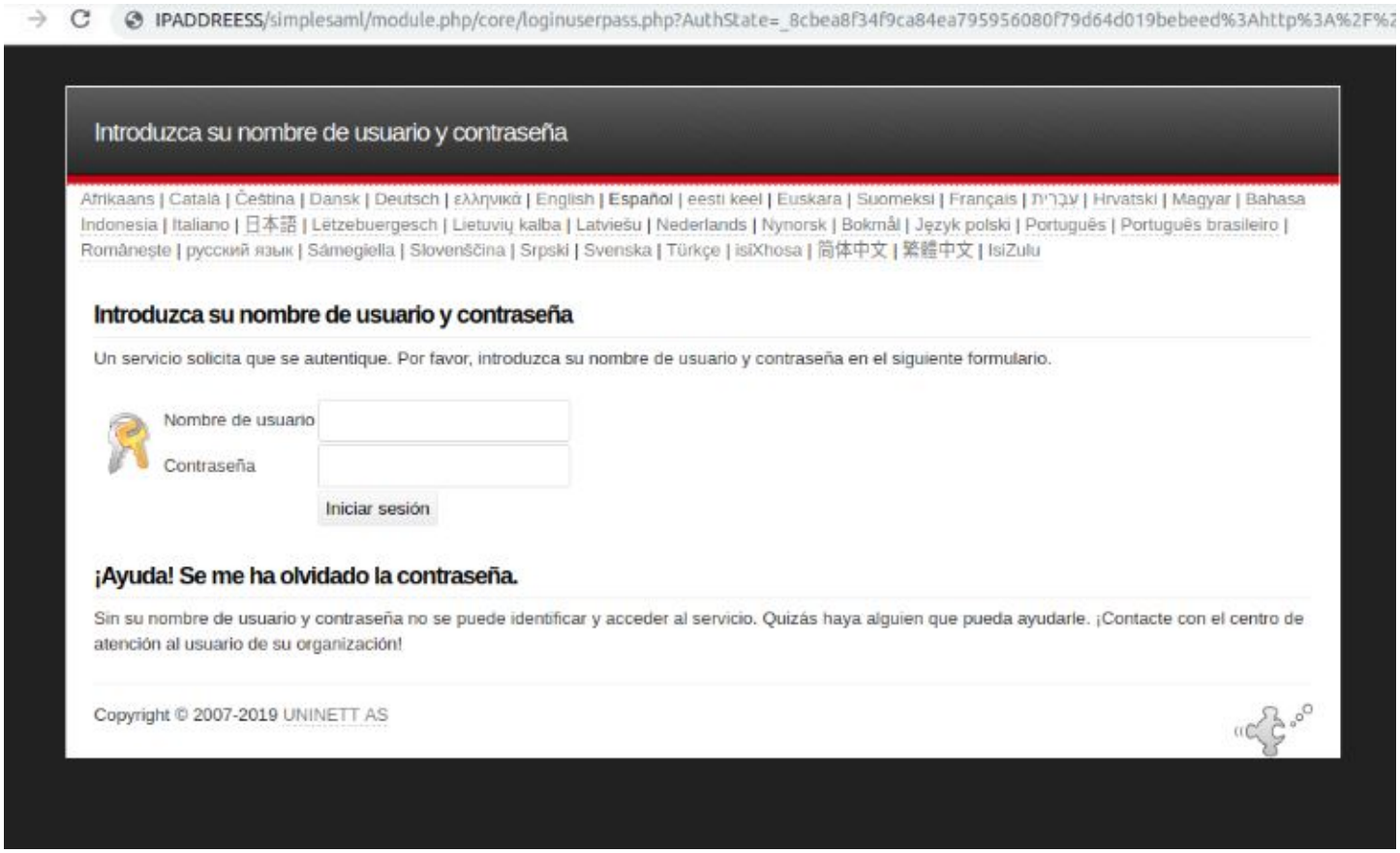
Vous devrez vous assurer que le fichier `/opt/simplesamlphp/lib/_autoload.php` existe.

Une fois simplesamlphp installé, vérifiez si le *login* fonctionne directement dans SAML. Pour ce faire, accédez à l'adresse IP suivante et sélectionnez la source d'authentification.

```
http://<IP_ADDRESS>/simplesaml/module.php/core/authenticate.php
```



Un écran *login* comme celui ci-dessous s'affiche, dans lequel vous devez saisir l'utilisateur SAML et le mot de passe que vous avez créé.



Si le *login* est correct, un écran récapitulatif avec tous les attributs de l'utilisateur s'affiche.

Le guide est également disponible à l'adresse suivante SimpleSAMLphp Service Provider QuickStart.

Configuration de votre fournisseur d'identité

Pour que les utilisateurs SAML soient générés correctement dans Pandora FMS, il est nécessaire de définir les attributs d'identification suivants qui apparaissent dans la configuration SAML pour chacun d'entre eux :

- Failback to local authentication : Si cette option est désactivée, aucun utilisateur n'existant pas dans SAML (à l'exception des utilisateurs de type superadministrateur) ne sera autorisé à se connecter. Si l'authentification par SAML échoue et que cette option est désactivée, la base de données du serveur ne sera pas interrogée.
- Automatically create remote users : Il créera automatiquement les utilisateurs lorsque vous vous connecterez pour la première fois à l'aide de SAML dans l'outil. S'il est désactivé, il doit être créé manuellement au préalable.
- SimpleSAML path : Définir le chemin d'accès au dossier dans lequel se trouve le répertoire `simplesamlphp`.
- SAML Source : Nom de la source SAML à laquelle les demandes doivent être adressées. Le nom doit correspondre à la source sélectionnée dans :

```
http://<IP_ADDRESS>/simplesaml/module.php/core/authenticate.php
```

- SAML user id attribute : Le champ récupéré de SAML à utiliser comme nom d'utilisateur (par ex. uid).
- SAML mail attribute : Le champ récupéré de SAML à utiliser comme courriel de l'utilisateur (par ex. email).
- SAML group name attribute : Le champ récupéré de SAML à utiliser comme groupe de l'utilisateur (par ex. group1PersonAffiliation).
- Profile attribute : Le champ récupéré de SAML à utiliser comme profil de groupe de l'utilisateur (par ex. urn:profile_example:Operator Read).
- Simple attribute / Multivalue attribute : Option permettant de choisir entre l'utilisation d'un attribut simple pour les champs Profil et Etiquette dans Pandora FMS ou d'un attribut multivaleur.

En cas de choix Simple attribute deux nouveaux champs apparaissent, intitulés Profile attribute et Tag attribute où seront sélectionnés les noms des attributs SAML qui coïncideront avec le nom du profil et de l'étiquette dans Pandora FMS lors de sa création.

Lorsque l'on sélectionne Multivalue attribute un attribut respectant ce format doit être utilisé :

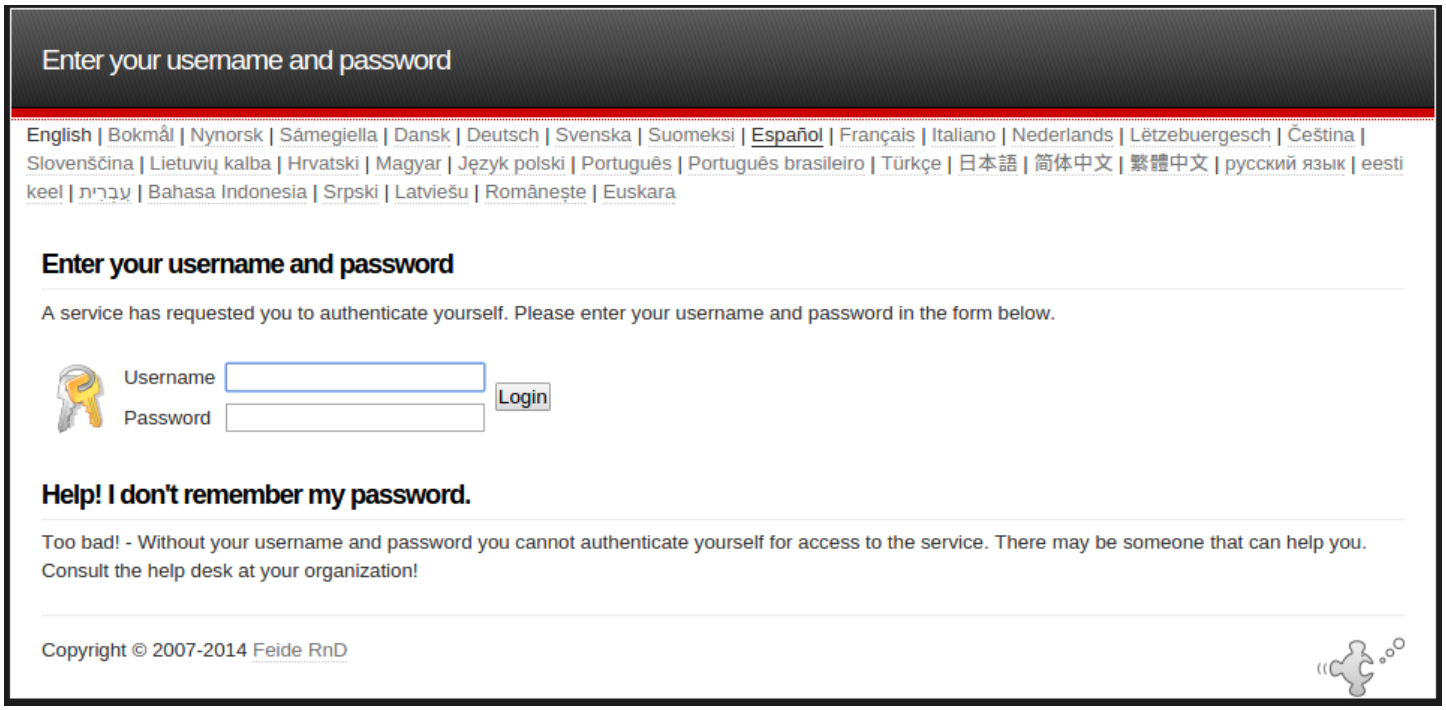
```
<Attribute Name="MULTIVALUE_ATTRIBUTE">
<AttributeValue>PREFIX:role:rolename</AttributeValue>
<AttributeValue>PREFIX:tag:tagname</AttributeValue>
</Attribute>
```

Une fois l'attribut créé dans le SAML et sélectionné de cette manière avec la configuration dans Pandora FMS, les paramètres suivants seront indiqués :

- SAML profiles and tag attribute : Nom de l'attribut multivaleur.
- SAML profile and tags prefix : Préfixe précédant le code *role* et *tag* dans la valeur de l'attribut. Dans le cas où il est `urn:pfms:role:< rolename >` et `urn:pfms:tag:` le préfixe doit être configuré `urn:pfms`.

Connexion

Vous devez vous rendre dans la console de Pandora FMS et cliquer sur le bouton *Login*. Vous serez redirigé vers le fournisseur d'identité.



Après une connexion réussie, vous serez redirigé vers la console Pandora FMS.

Retour à l'index de la documentation de Pandora FMS