Mise en place de XACML

Yannick Chevalier
Université de Toulouse
IUP NTIE M2 2012-2013

Plan

But

- Mettre en place un PDP xacml
- Récupérer les décisions de ce PDP
- Mettre en place un PAP xacml
- Ajouter/enlever des politiques

Pré-requis

Être `root` sur une machine Linux avec Debian/Ubuntu avec un terminal et `bash`

Plan

TÉLÉCHARGEMENT

VARIABLES D'ENVIRONNEMENT

- On va utiliser la version 1.6.2
- On va faire une installation `standalone` (en dehors de Tomcat)

DANS LE TERMINAL

```
export AXIS_VERSION=1.6.2
export AXIS="axis2-${AXIS_VERSION}"
wget http://apache.crihan.fr/dist/axis/axis2/\
  java/core/${AXIS_VERSION}/${AXIS}-war.zip
```

Installation de Java

Dans le terminal

```
export JDK_VERSION=6
sudo apt-get install \
  openjdk-${JDK_VERSION}-jdk ant maven2
export JAVA_HOME=$(readlink -f \
  /usr/bin/java | sed "s:bin/java::")
```

Commentaires

- `readlink` suit une séquence de liens symboliques jusqu'à arriver à un vrai fichier
- `sed` enlève la fin du nom du vrai java pour avoir le répertoire `JAVA_HOME`
- On aurait pu utiliser dirname et xargs à la place

Création d'un répertoire dédié à Axis

Dans le terminal

```
export AXIS_DIR=/var/www-axis
sudo mkdir -p "${AXIS_DIR}"
sudo chown -R root:root "${AXIS_DIR}"
```

Copie d'Axis

Dans le terminal

```
sudo cp ${AXIS}-bin.zip ${AXIS_DIR}
cd ${AXIS_DIR}
sudo unzip ${AXIS}-bin.zip
sudo \rm ${AXIS}-bin.zip
```

Configuration d'Axis

Fichier .bashrc

Variables d'environment

- Axis a un fichier de variables d'environnement (setenv.sh)
- Mais on veut aussi pouvoir récupérer AXIS_DIR, etc.
- Il faut être root au moment de l'ouverture de la redirection, ce qui oblige à utiliser `bash -c`

Dans le terminal

```
sudo bash -c \
"echo \"export JAVA_HOME=${JAVA_HOME}\" \
>> ${AXIS_DIR}/.bashrc"
sudo bash -c \
"echo \"export AXIS_HOME=${AXIS_DIR}/${AXIS}\" \
>> ${AXIS_DIR}/.bashrc"
sudo bash -c \
"echo \"export PATH=\\\${AXIS_HOME}/bin:\\\${PATH}\" \
>> ${AXIS_DIR}/.bashrc"
```

Recherche d'un port libre pour le serveur Axis2

Commentaires

- Par défaut, Axis2 se met sur le port 8080
- Comme Tomcat...
- On part de ce numéro de port, et on configure le serveur sur le premier port libre
- Attention, risque de conflit si Tomcat est configuré sur 8080 mais n'est pas lancé
- On utilise `nc` pour tester si un serveur répond sur un port donné

Dans le terminal

```
while nc localhost "${port}" -z > /dev/null; do
  port=$((${port}+1))
done
```

Configuration d'Axis

Fichier conf/axis2.xml

Dans le terminal

```
sudo sed -i -e \
  's/8080/"${port}"/g' \
  ${AXIS_DIR}/${AXIS}/conf/axis2.xml
```

Et on termine la configuration du bashrc :

Dans le terminal

```
sudo bash -c \
"echo \"export AXIS2_ADDR=\\\"http://localhost:${port}/axis2/services\\\
>> ${AXIS_DIR}/.bashrc"
sudo bash -c \
"echo \"source ${AXIS_DIR}/${AXIS}/bin/setenv.sh\"\
>> ${AXIS_DIR}/.bashrc"
```

Configuration d'Axis

Fichier conf/axis2.xml

Dans le terminal

```
sudo sed -i -e \
  's/8080/"${port}"/g' \
  ${AXIS_DIR}/${AXIS}/conf/axis2.xml
```

Et on termine la configuration du bashrc :

Dans le terminal

```
sudo bash -c \
"echo \"export AXIS2_ADDR=\\\"http://localhost:${port}/axis2/services\\\
>> ${AXIS_DIR}/.bashrc"
sudo bash -c \
"echo \"source ${AXIS_DIR}/${AXIS}/bin/setenv.sh\"\
>> ${AXIS_DIR}/.bashrc"
```

Plan

UTILISATION DES ACLS

SUIVANT LES VERSIONS

- Regarder dans le fichier `/etc/fstab`
- Il faut qu'une des options de la partition contenant axis soit acl :

```
UUID=xxx / ext4 errors=remount-ro,acl 0 1
```

- Si ce n'est pas le cas, éditer ce fichier et redémarrer
- (si c'est une sous-partition, il suffit de la démonter et la remonter)

Création d'un client pour Axis

Phase de test

On utilise un script bash qui :

- Fait des requêtes SOAP vers le serveur Axis
- Affiche la réponse

Ce script est basé sur curl

Dans le terminal

```
sudo wget \
http://www.irit.fr/~Yannick.Chevalier/soap_query
mv soap_query "${AXIS_DIR}/${AXIS}/bin/"
```

Utilisation en production

En vrai :

- Rappel : le PEP est l'application
- Dans l'application, il faut :
  - créer les requêtes SOAP
  - les envoyer
  - lire le document XML contenu dans la réponse
- On a tout intérêt à écrire une classe dédiée...

Plan

Ajouter un administrateur Axis (1/3)

2 phases :

- Un premier script, lancé par un administrateur existant ou l'utilisateur axis2, donne les droits à un utilisateur passé en argument
- Un second script, lancé par le nouvel administrateur, change sa configuration pour lui permettre d'utiliser facilement les scripts d'axis

Ajouter un administrateur Axis (2/3)

On crée un script axis_add_admin.sh

Dans le terminal

```
sudo bash -c \
"cat > ${AXIS_DIR}/${AXIS}/bin/axis_add_admin.sh"  <<'EOF'
#! /bin/bash

user=${1}
if id "${user}" > /dev/null ; then
    setfacl -R -m u:${user}:rwx AXIS_DIR
else
    exit 1
fi
exit 0
EOF
sudo sed -i -e 's+AXIS_DIR+'"${AXIS_DIR}"'+g' \
  ${AXIS_DIR}/${AXIS}/bin/axis_add_admin.sh
```

Ajouter un administrateur Axis (3/3)

On crée un script axis_become_admin.sh

Dans le terminal

```
sudo bash -c "sed -e \"s|AXIS_DIR|${AXIS_DIR}|g\" \
> /var/www-axis/axis2-1.6.2/bin/axis_become_admin.sh"  <<'EOF'
#! /bin/bash
cat >> ${HOME}/.bashrc <<USER_BASH_RC
function axis_admin () {
    source AXIS_DIR/.bashrc
}
USER_BASH_RC
exit 0
EOF
sudo chmod 700 ${AXIS_DIR}/${AXIS}/bin/axis_add_admin.sh \
${AXIS_DIR}/${AXIS}/bin/axis_become_admin.sh
```

Enregistrement comme administrateur

Dans le terminal

```
sudo ${AXIS_DIR}/${AXIS}/bin/axis_add_admin.sh ${USER}
bash /var/www-axis/axis2-1.6.2/bin/axis_become_admin.sh
```

Création d'un utilisateur Axis

Partie variant suivant la distribution

Dans le terminal

```
if id axis2 > /dev/null 2>&1; then
  echo "Pas de cr{\'e}ation d'un utilisateur axis"
else
  sudo /usr/sbin/useradd -r axis2 \
    -N -G www-data -s /bin/bash -d ${AXIS_DIR}
  sudo chown -R axis2:www-data "${AXIS_DIR}"
fi
```

Commentaires

- On teste d'abord si l'utilisateur existe déjà avec `id`
- `-N -G www-data` permet de ne pas créer de groupe spécifique à l'utilisateur axis2, et d'ajouter cet utilisateur directement au groupe `www-data`

Script pour les clients

Dans le terminal

```
sudo bash -c "cat > ${AXIS_DIR}/${AXIS}/bin/axis_become_client.sh" \
  <<EOF
#! /bin/bash
if [ ! -d "\${HOME}"/bin ] ; then
  mkdir "\${HOME}"/bin
fi
cp ${AXIS_DIR}/${AXIS}/bin/soap_query "\${HOME}"/bin
if ! type soap_query ; then
  echo "export PATH=\"\${HOME}\"/bin:\${PATH}" >> "\${HOME}"/.bashrc
fi
EOF
sudo chmod 755 "${AXIS_DIR}/${AXIS}/bin/axis_become_client.sh"
```

INSTALLATION RAPIDE

DANS LE TERMINAL

```
\curl -L \
http://www.irit.fr/~Yannick.Chevalier/\
install_axis2_standalone.sh \
| bash
```

Plan

INSTALLATION RAPIDE

PRÉ-REQUIS

- Il faut avoir installé axis2
- Il faut être administrateur et client axis2

DANS LE TERMINAL

```
cd ~/bin
wget http://www.irit.fr/~Yannick.Chevalier/xacmllight.sh
```

Notes

Problèmes de configurations

- On va utiliser XACMLLight 2.2
- Les messages de tests sont dépassés

  On les ré-écrits
- Le WSDL n'est pas à jour

  On dit à Axis de le générer automatiquement

Facilités d'utilisation

- On va créer des fonctions qui appellent directement le PDP et le PAP
- Cela suppose qu'on est client d'Axis (utilisation de `soap_query`)

Utilisation

Installation (-i)

- Télécharge xacmllight
- L'installe et le configure automatiquement
- Nécessite d'être administrateur ou axis2

Utilisation (-c)

- Change la configuration de l'utilisateur lançant le script
- Crée un fichier `~/.xacml_clientrc` contenant les fonctions liées à xacml
- Ajoute dans `~/.bashrc` une fonction `use_xacml` qui charge ces fonctions

Aide (-h)

Décrit les 2 options supplémentaires (-a et -v)

Plan

VÉRIFICATION DE L'INSTALLATION

À PARTIR DU NAVIGATEUR

- Ouvrir la page `http://localhost:8081/`
- Vérifier que le PDP et le PAP sont listés parmi les services disponibles
- En profiter pour lire les opérations disponibles

Requêtes de test

Répertoire de test

- Le répertoire de test est dans le répertoire de téléchargement de xacmllight
- Il contient des politiques et des requêtes au bon format

Exercice

- Tester les requêtes fournies
- Essayer d'écrire un nouveau fichier de politique et de le soumettre au PAP
- Tester que cette nouvelle politique est prise en compte