

Author: Eric Engstfeld

Date: 3 de July, 2015

Gateway

Abstract

La finalidad de este documento consiste en exponer cómo está construido el componente Gateway, los pasos para su instalación, su adecuada configuración y detallar sus funcionalidades principales y características para una futura extensión y reutilización por parte de otros componentes. Al final del mismo se encontrará una sección de glosario explicando aquellos términos técnicos que ameritan aclaración y a su vez otra de contacto con los datos de sus desarrolladores en caso de dudas o sugerencias.

Index

1. [Introducción](#)
2. [Librerías](#)
3. [Pre-Requisitos](#)
4. [Instalación](#)
5. [Consideraciones especiales](#)
 - [Instalación en ambiente productivo](#)
 - [Instalación de M2Crypto en MAC](#)
6. [Glosario](#)
7. [Contacto](#)

Introducción

El Gateway es un componente escrito en Python 2.7 diseñado para ser parte de

la solución general de adaptar una aplicación web basada en servicios REST a la arquitectura provista por ANSES, que impone como normativa soportar comunicación SOAP y pasar por un agente de seguridad llamado Director a la hora de consultar los servicios de backend. El mismo a través de configuraciones toma los servicios, módulos de la GUI y roles de la aplicación para realizar mappings con sus funcionalidades y rechazar o permitir los diferentes requerimientos de los usuarios. Este agente expone también un servicio para recuperar esta matriz de roles por funcionalidades y consultarla para luego utilizarse en la aplicación. En resumen, el Gateway toma una aplicación web, la levanta, expone la forma de logueo integrada con el Autenticador (para obtener datos de usuario y credenciales específicas de la institución) monitorea todos los request que salen y envía cada uno de ellos al servicio correspondiente de backend aplicando las políticas de seguridad necesarias por el Director, entre ellas: validación de TOKEN e inyección de HEADERS. Esta lógica es implementada a través de configuraciones de ruteo en base a la URL y método del servicio solicitado. Adicionalmente la aplicación expone un servicio REST para recuperar la matriz de roles desde el Director y parsear el dato por medio de una función configurable para adaptarlos a la necesidad de la aplicación sin tocar código.

Librerías

El lenguaje utilizado es Python 2.7 conteniendo a su vez las siguientes librerías disponibles en su repositorio (<https://pypi.python.org/>):

- [Flask](#)
- [M2Crypto](#)
- [flask_cors](#)
- [httplib2](#)
- [pysimplesoap](#)
- [dicttoxml](#)

Pre-Requisitos

1. Para ambiente productivo:

- Python 2.7
- Apache2
- Conexión con el Director

2. Para ambiente de desarrollo:

- Python 2.7
- Instancia de SOAP Server corriendo

En cuanto al tamaño del servidor, debe tenerse en cuenta la dimensión de la aplicación que se está levantado. Ya que el gateway en sí casi no posee lógica.

Instalación

Ingresar al directorio raíz del proyecto gateway y ejecutar el setup.py para instalar las librerías:

```
python setup.py build
python setup.py develop
```

Una vez instaladas las librerías podremos ejecutar el código, pero antes de ello debemos armar nuestro propio archivo de configuración para adaptarlo a nuestro entorno. Copiamos alguno de ejemplo desde el directorio /etc y lo editamos:

```
cp etc/gateway.cfg /my/project/configuration/path/
vim /my/project/configuration/path/gateway.cfg
```

A continuación detallaremos cada una de las secciones del mismo para facilitar y hacer más amena esta tarea:

~~~~~

## GENERAL CONFIGURATIONS

PORT=4500 -> Puerto donde correrá la aplicación APPLICATION="EIMEO" -> Nombre representativo de la aplicación a levantar  
HTML\_FOLDER="/home/b996031/moorea/sources/moorea\_imanager/html/" -> Dirección del FRONT que se desea correr  
TOKEN\_ATTR\_CN="nombre" -> Nombre del atributo CN en el TOKEN de ANSES  
TOKEN\_ATTR\_ORGANIZATION\_ID="oficina" -> Nombre del atributo ORGANIZATION\_ID en el TOKEN de ANSES  
MAIL\_ATTR="email" -> Nombre del atributo MAIL en el token de ANSES  
FIXED\_ORGANIZATION\_ID="TEST" -> ORGANIZATION\_ID por defecto (en caso de no encontrarla en el TOKEN)  
SECURE\_SERVICES\_PATH="security/token/create" -> Servicio de seguridad a utilizar en caso de ser requerido por el BACKEND  
SECURE\_SERVICES\_ENABLED=True -> Habilitar o deshabilitar soporte de servicios seguros (debe existir el servicio CreateSessionToken/POST en el soap server)  
INITIAL\_CONFIGURATION\_ENABLED=True -> Habilitar o deshabilitar la carga inicial de la configuración al renderizar el index.html por primera vez (debe existir el servicio GetConfig en el soap server)  
DEV\_MODE=False -> Habilitar o deshabilitar modo development para realizar pruebas locales  
DEV\_MODE\_USER={"one\_shoot":False, "uid":"dev\_mode", "email":"dev\_user@moorea.io", "organization\_id": "test", "roles":["Administrador"], "cn":"dev\_mode"} -> Datos de usuario a utilizar en modo development  
DEV\_MODE\_TOKEN={"token":"UN\_TOKEN", "sign":"UN\_SIGN", "ACTION":"un\_action"} -> Datos del token a utilizar en modo development  
WILDCARD="" -> Comodín utilizado en los patrones de ruteo (/api/users/)

# SERVER SOAP CONFIGURATION

Datos de conexión al servidor SOAP que expondrá el BACKEND. En caso de funcionar tras el Director, aquí debe estar configurado

```
WSDL='http://localhost:4501/soap/retrieve?wsdl'  
#WSDL="http://ansesarg.anses.gov.ar:4501/soap/retrieve?  
wsdl"  
LOGIN_URL="http://labprueba3/garquitectura/aplicaciones  
/arg.aspx"  
#LOCATION="http://ansesarqdir01.anses.gov.ar:81/Directo  
rSOA/director.svc/soap11/retrieve"  
LOCATION="http://ansesarg.anses.gov.ar:4501/soap/retrie  
ve"  
ACTION="http://ansesarg.anses.gov.ar/"  
NAMESPACE="http://ansesarg.anses.gov.ar"  
CREDENTIALS_XMLNS="http://director.anses.gov.ar"  
EXCEPTIONS=False  
SOAP_NS='soapenv'  
TRACE=True  
NS="ans"  
PROXY={}
```

## ROLES MATRIX SERVICE DATA

Configuración del servicio que nos devolverá la matriz de ROLES, debe exponer protocolo SOAP

```
ANSES_ROLES_MATRIX_WSDL="http://ansesarqdir01.anses.gov  
.ar:8023/DirectorSOA/GrantForSystemGroup.svc?wsdl"  
ANSES_ROLES_MATRIX_EXCEPTIONS=False  
ANSES_ROLES_MATRIX_SOAP_NS="soapenv"  
ANSES_ROLES_MATRIX_TRACE=True  
ANSES_ROLES_MATRIX_NS="ans"  
ANSES_ROLES_MATRIX_PROXY={}  
ANSES_ROLES_MATRIX_PARSER=lambda matrix:  
[menu["accion"] for menu in matrix] -> Función a  
ejecutar para parsear la respuesta del servicio. Aquí  
es donde lo adapta a las necesidades de su App.
```

## SECURITY CONFIGURATION

Configuración de validaciones al TOKEN y SIGN provisto por el autenticador. Se puede habilitar o deshabilitar y configurar los distintos

mensajes de errores.

```
ANSES_TOKEN_VALIDATIONS_ENABLED = True
VALIDATION_SIGN_CERT_PATH="/Users/eric/Development/cert_
_ances.crt" -> Aquí debe ingresar la dirección del
certificado utilizado para validar el SIGN
VALIDATION_SIGN_MSG="La firma no es valida"
VALIDATION_IP_MSG="Su IP no esta habilitada para
utilizar la aplicacion"
VALIDATION_EXPIRATION_MSG="Su token ha expirado"
```

## SERVICES MAPPING

Configuración de ruteo de servicios. Por defecto la aplicación asumirá que se trata de un componente estático a renderizar. Por ello, debe configurar aquí todos los request REST que saldrán del FRONT para ser reconocidos y proxiadados al servicio de BACKEND correspondiente

```
SERVICES=[{
    'pattern':'config/as_array', -> Patrón
de URL del servicio requerido, puede contener
WILDCARDS en caso de tratarse de una variable
    'method':'GET', -> Método HTTP mapeado
a la URL configurada
    'soap_method':'GetConfigAsArray', ->
Método SOAP que se deberá invocar del lado del
SOAPSERVER
}, {
    'pattern':'api/users/*',
    'method':'GET',
    'soap_method':'Alive',
}]
```

Finalmente podremos correr nuestra aplicación exportando primero la variable de ambiente indicando la configuración a utilizar y luego ejecutando el componente:

```
export
GATEWAY_SETTINGS=/my/proyect/configuration/path/gateway
.cfg
python src/runserver.py
```

Deberíamos ver el siguiente output:

```
* Running on http://0.0.0.0:3000/ (Press CTRL+C to
quit)
* Restarting with stat
```

## Consideraciones especiales

En el siguiente apartado se encontrarán ciertas consideraciones especiales o problemas comunes a modo de consulta en caso de que se tope con alguna de ellas.

## Instalación en ambiente productivo

---

En un ambiente productivo debe tenerse en cuenta que el componente debe correr en un WEB SERVER. En este caso tomaremos como ejemplo [Apache2](#). Dentro de la raíz del proyecto encontrará un archivo .wsgi listo para ser integrado y configurado en el mismo.

## Instalación de M2Crypto en MAC

---

Se preguntará por que este título en el apartado. Pues bien, esta librería trae problemas a la hora de instalarla en MAC, por lo que a continuación detallaremos su instalación en este ambiente. Primero, no debemos usar BREW al instalarla ya que nos instalará la version 3.0.5 y necesitamos la 3.0.4, por lo tanto procederemos a descargar la correcta versión y su instalación manual:

- Descargar `swig` 3.0.4  
(<http://sourceforge.net/projects/swig/files/swig/swig-3.0.4/>)
- En el directorio descargado correr `./configure` Luego correr `make`
- Luego correr `make install`

## Glosario

- Autenticador: Módulo de autenticación provisto por ANSES. Funciona haciendo un POST con un TOKEN, SIGN y action al punto de entrada de la aplicación para que ella lo parsee y tome los datos del usuario que está ingresando. Estos datos y estos usuarios se hayan en el Active Directory de la institución, por lo que está integrado con los usuarios de las PCs y asimismo con la seguridad integrada soportada por los navegadores Chrome e Internet Explorer.
- Director: Agente de seguridad que controla todos los llamados hacia los servicios de BACKEND desde las distintas aplicaciones de FRONT. Trabaja con el protocolo SOAP y posee una aplicación con fines de configuración asociada en la cual se pueden configurar las distintas aplicaciones con sus servicios, roles, funcionalidades y módulos de la GUI (matriz de permisos/roles)

- Soap Server: El SOAP SERVER es otro componente dentro del mismo repositorio y solución que, junto al GATEWAY, proveen el módulo de seguridad completo para adaptar sus aplicaciones FRONT al esquema de seguridad de ANSES. Para más información consulte el README.md en la raíz de su directorio (source/soap-server-dynamic/)

## Contacto

Si desea contactarse con el equipo por alguna duda o sugerencia puede realizarlo a través del siguiente e-mail: [eric@moorea.io](mailto:eric@moorea.io)