AGESIC

Trazabilidad - backoffice

Manual de Instalación

Desarrollo

Versión 3

Histórico de revisiones			
FECHA	VERSIÓN	DESCRIPCIÓN	AUTOR
05/10/2015	1.0	Creación del documento	Valentina Rodríguez
22/12/2015	1.1	Actualización fase 2	Valentina Rodríguez
11/02/2016	1.2	Actualización fase 3	Valentina Rodríguez
17/03/2016	2	Actualización	Valentina Rodríguez
09/05/2016	3	Correcciones en base a comentarios de Agesic	Valentina Rodríguez

TABLA DE CONTENIDOS

1 Supuestos

- Instalación de postgres aceptando conexiones desde el servidor de aplicaciones.
- Instalación de WildFly 8.2.1 Final.
- En caso de existir un dominio jboss, todas las instancias de servidor del server-group deben tener un nombre distinto

2 Configuración de ambiente:

- Agregar módulo postgres en ambos servidores:
    - <WildFly-8.2.1>/modules/system/layers/base/org/postgresql
- Agregar datasource, ejemplo anexo 1.
- Agregar ears al servidor de Backend (itramites-bruto.ear, itramites-estructurado.ear, itramites-transferencia.ear, itramites-integracion.ear). En la consola de wildfly, Deployments/Add/<seleccionar archivo.ear>
- Agregar ear al servidor de Frontend (itramites-frontend.ear).
- Asociar ear al server group.
- Configurar el WSDLHost del subsistema WebServices (dentro de la consola sería Configuracion –> Web –> Web Service.
- En la consola de administración de WildFly ir al profile que corresponda y agregar una nueva system propertie con key:

PRODUCCION:

- APP02 y APP03 – BACKEND:

Variables para configuración de guía de trámites

- http.nonProxyHosts – value: *.red.uy|localhost
- http.proxyHost – value: 10.240.15.125
- http.proxyPort: value: 3128

Variable de configuración global:

- RUNTIME_ENVIRONMENT_TYPE - value: PRODUCCION

- APP01 – FRONTEND:

Variables para COESYS:

- idp.sig.url – value: https://eid.portal.gub.uy/idp/profile/SAML2/Redirect/SSO

El valor corresponde a la url del IDP de COESYS.

- idp-logout.url – value: https://eid.portal.gub.uy/idp/profile/SAML2/Redirect/SLO

El valor que corresponda a la url de logout de COESYS

- itramites-frontend-post.url – value: https://trazabilidad.pge.red.uy/itramites-frontend/

El valor corresponde a la url pública de la aplicación de itramites

- sp-logout.url – value: https://trazabilidad.pge.red.uy/itramites-frontend/GLO=true

El valor corresponde a la url de inicio de la aplicación.

- saml-authentication-handler - value: uy.gub.agesic.itramites.cda.handler.CDASAML2AuthenticationHandler
- signing-key-alias

El valor corresponde al alias del certificado a usar contra COESYS dentro del keystore.

- signing-key-pass

El valor correspondiente a la clave del certificado

- AJUSTE_RELOJ_CDA_MILLIS - value="60000"

Variable de configuración global:

- RUNTIME_ENVIRONMENT_TYPE - value: PRODUCCION

- Variables infinispan:
    - Cache containers:

      Name: entidades

      Start: EAGER

      JNDI Name: java:/infinispan/container/entidades

PREPRODUCCION:

- APP02 y APP03 – BACKEND:

Variables para configuración de guía de trámites

- http.nonProxyHosts – value: *.red.uy|localhost
- http.proxyHost – value: 10.255.15.125
- http.proxyPort: value: 3128

Variable de configuración global:

- RUNTIME_ENVIRONMENT_TYPE - value: PREPROD

- APP01 – FRONTEND:

Variables para COESYS:

- idp.sig.url – value: https://test-eid.portal.gub.uy/idp/profile/SAML2/Redirect/SSO

El valor corresponde a la url del IDP de COESYS.

- idp-logout.url – value: https://test-eid.portal.gub.uy/idp/profile/SAML2/Redirect/SLO

El valor que corresponda a la url de logout de COESYS

- **itramites-frontend-post.url –** value: https://preprod.trazabilidad.pge.red.uy/itramites-frontend/

El valor corresponde a la url pública de la aplicación de itramites

- **sp-logout.url –** value: https://preprod.itramites.pge.red.uy/itramites-frontend/GLO=true

El valor corresponde a la url de inicio de la aplicación.

- **saml-authentication-handler -** value: uy.gub.agesic.itramites.cda.handler.CDASAML2AuthenticationHandler
- **signing-key-alias**

El valor corresponde al alias del certificado a usar contra COESYS dentro del keystore.

- **signing-key-pass**

El valor correspondiente a la clave del certificado

- **AJUSTE_RELOJ_CDA_MILLIS** - value="60000"

Variable de configuración global:

- **RUNTIME_ENVIRONMENT_TYPE -** value**: PREPROD**
  - Variables infinispan:
    - **Cache containers:**

Name: entidades

Start: EAGER

JNDI Name: java:/infinispan/container/entidades

3 Configuración de Base de datos:

1. Creación de Rol
2. Crear base de datos: itramitesdb. (create database itramitesdb;)

3. Asociar owner de base al rol creado en el punto 1.
4. Levantar dump de la base. (psql -f <dump.sql> itramitesdb)
5. Modificar en el archivo: postgresql.conf la línea "max_prepared_transactions" para que quede descomentada, y de la siguiente manera:
    - max_prepared_transactions = <Valor dependiente del dimensionamiento>

NOTA: Asegurarse que se corra a diariamente a las 00hs el script que actualiza la vista itramitesestructuradodb.fechas_cabezal

4 Configuración de Proceso de Transferencia:

1. Editar el archivo itramites-transferencia-ear.ear/lib/itramites-transferencia-business.jar/transferencia-config.properties
    - tamanio.bloque.validacion=<<tamaño-bloque-validacion>>
    - tamanio.bloque.transferencia=<<tamaño-bloque-transferencia>>

1. Configurar la modalidad de transferencia, mediante la system property bloques.transferencia.persistentes.habilitados
    - false para modalidad convencional
    - true para modalidad persistente

5 Configuración de Mail:

1. Editar el archivo itramites-transferencia-ear.ear/lib/itramites-transferencia-business.jar/prod-mail.properties

mail.smtp.from=<<from>> -ejemplo:noreply@agesic.gub.uy
mail.smtp.host=<<servidor-smtp>> -ejemplo:smtp.agesic.red.uy
mail.smtp.port=<<puerto-smtp>> -ejemplo:25
mail.smtp.user=<<usuario-mail>> -ejemplo:noreply
mail.smtp.password=<<password-usuario>>

mail.debug=true
mail.smtp.auth=true

6 Configuración de COESYS:

1. Habilitar el security domain SP para SAML (ver anexo 3 - configuración SAML)
2. Colocar el keystore con el certificado válido para comunicarse con COESYS dentro del directorio itramites-frontend-ear.ear/itramites-frontend-war.war/WEB-INF/classes
3. Ver referencia a variable de ambiente en el punto 2. Configuración de ambiente.

Notas:

- La ruta del keystore es relativa al directorio WEB-INF/classes / (punto 3.c)
- La configuración de la url del identityProvider y ServiceProvider es altamente sensible, y debe coincidir exactamente con lo que hay configurado. El mero hecho de agregar/quitar una barra al final de la cadena de caracteres hace que la validación falle

7 Configuración emisor de trazas:

1. Obtener el certificado para el emisor de trazas (AGESIC lo consigue), keystore y truststore para conexión SSL con PDI
2. Es necesario reemplazar el archivo itramites-frontend-ear.ear/itramites-frontend-ejb.jar/lineaService.wsdl con el devuelto al momento de publicar el servicio de líneas en la plataforma (debería ser suficiente con actualizar la ruta de soap:address)
3. Editar el archivo itramites-frontend-ear.ear/itramites-frontend-ejb.jar/prod-frontend.properties, corrigiendo el valor "ws.url" con el valor de la url lógica del servicio de líneas en PDI
4. Editar en el archivo itramites-frontend-ear.ear/itramites-frontend-ejb.jar/pge-config.xml las siguientes entradas:

   <Property Key="Role" Value="<<ROL_PDI_EMISOR_TRAZAS>>"/>

   <Property Key="Username" Value="<<USERNAME_STS>>"/>

   <Auth Key="KeyStoreURL" Value="keystore/<<nombre-archivo-keystore>>"/>

   <Auth Key="KeyStorePass" Value="<<password-keystore>>"/>

   <Auth Key="KeyStoreAlias" Value="<<alias-certificado-en-keystore>>"/>

   <Auth Key="SSLKeyStoreURL" Value="keystore/<<nombre-archivo-ssl-keystore>>"/>

   <Auth Key="SSLKeyStorePass" Value="<<password-keystore-ssl>>"/>

   <Auth Key="TrustStoreURL" Value="keystore/<<nombre-archivo-truststore>>"/>

   <Auth Key="TrustStorePass" Value="<<password-truststore>>"/>

5. Editar el archivo itramites-frontend-ear.ear/itramites-frontend-ejb.jar/prod-frontend.properties

   ws.url=<<url del servicio>>

Nota: Los keyStore/truststore tienen que estar configurados exactamente igual que si se fuera a utilizar el conector PGE. Prod-frontend.properties tiene otras propiedades pero están no deberian cambiarse.

8 ANEXOS:

a. Datasources

a) 5 Datasources non-XA

- Name: itramitesbrutoDS
- JNDI Name: java:/datasources/itramitesbrutoDS
- Driver: org.postgresql.Driver
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user
- Password: db_password

- Name: itramitesestructuradoDS
- JNDI Name: java:/datasources/itramitesestructuradoDS
- Driver: org.postgresql.Driver
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user
- Password: db_password

- Name: itramitesfrontendDS
- JNDI Name: java:/datasources/itramitesfrontendDS
- Driver: org.postgresql.Driver
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user
- Password: db_password

- Name: itramitesIntegracionDS
- JNDI Name: java:/datasources/itramitesIntegracionDS

- Driver: org.postgresql.Driver
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user
- Password: db_password

- Name: itramitesquartzDS
- JNDI Name: java:/datasources/itramitesquartzDS
- Driver: org.postgresql.Driver
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user
- Password: db_password

b) 2 Datasources XA

- Name: itramitesbrutoXADS
- JNDI Name: java:/datasources/itramitesbrutoXADS
- Driver: org.postgresql.xa.PGXADataSource
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user (mismo al de bruto non-xa)
- Password: db_password

- Name: itramitesestructuradoXADS
- JNDI Name: java:/datasources/itramitesestructuradoXADS
- Driver: org.postgresql.xa.PGXADataSource
- Connection URL: jdbc:postgresql://<db_host>:<port>/itramitesdb
- Username: schema_user (mismo al de estructurado non-xa)
- Password: db_password

b.

Nota:

Todos los datasources deben tener la siguiente configuración adicional:

<new-connection-sql>SET search_path TO <<nombre-schema-correspondiente>>;</new-connection-sql>

```
<validation>
        <valid-connection-checker class-name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLValidConnectionChecker"/>
        <check-valid-connection-sql>select 1</check-valid-connection-sql>
        <validate-on-match>true</validate-on-match>
        <background-validation>false</background-validation>
        <exception-sorter class-name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLExceptionSorter"/>
</validation>
<timeout>
        <set-tx-query-timeout>false</set-tx-query-timeout>
        <blocking-timeout-millis>0</blocking-timeout-millis>
        <idle-timeout-minutes>30</idle-timeout-minutes>
        <query-timeout>0</query-timeout>
        <use-try-lock>0</use-try-lock>
        <allocation-retry>0</allocation-retry>
        <allocation-retry-wait-millis>0</allocation-retry-wait-millis>
</timeout>
```

c. Habilitación de autenticación SAML

Es necesario editar el archivo domain.xml, y en el profile correspondiente (opcionalmente en todos los profiles), agregar dentro de la sección:

```
<subsystem xmlns="urn:jboss:domain:security:1.1">
```

dentro del grupo:

```
<security-domains>
```

El siguiente bloque:

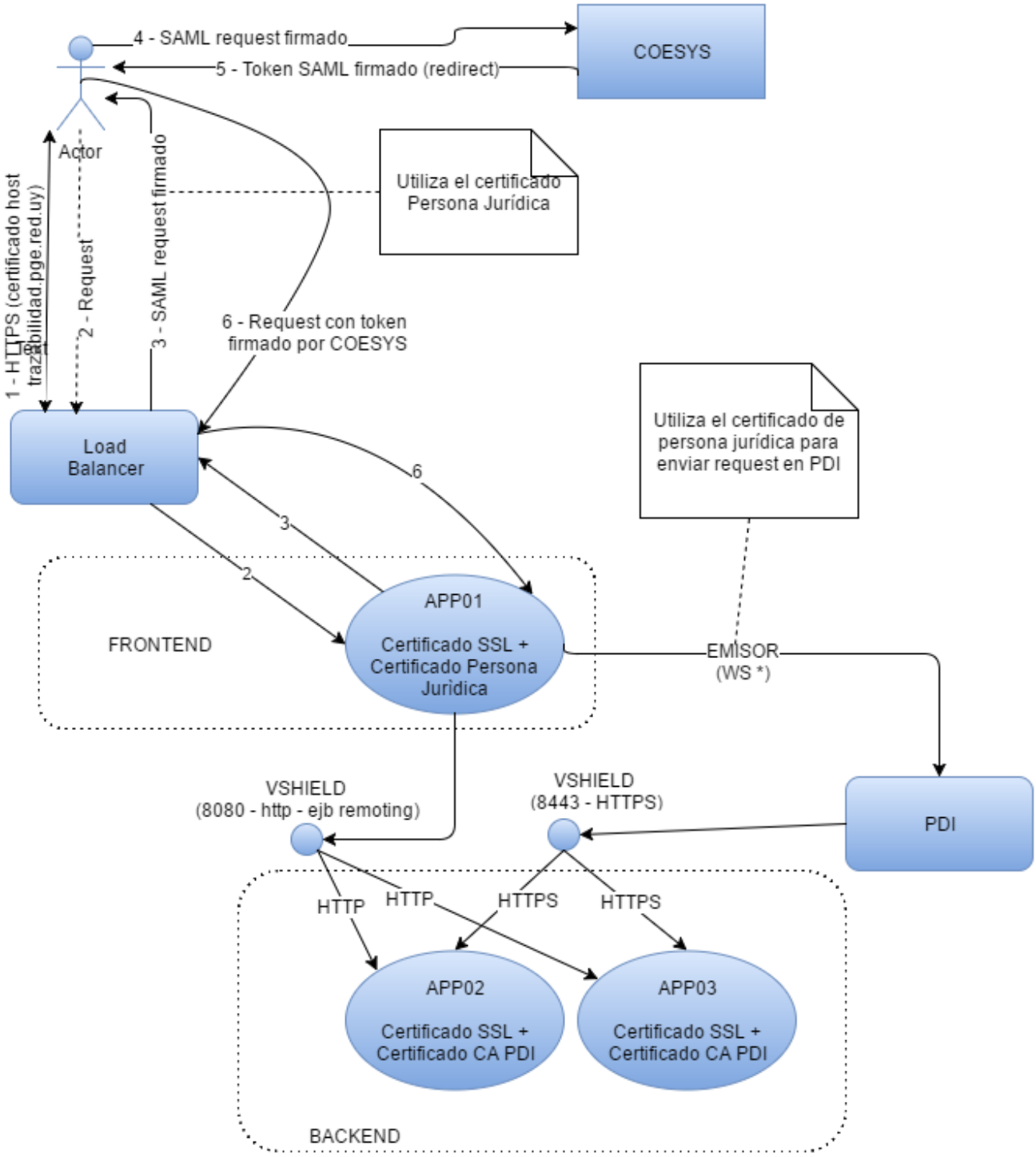
```
<security-domain name="sp" cache-type="default">
    <authentication>
      <login-module
code="org.picketlink.identity.federation.bindings.jboss.auth.SAML2LoginModule" flag="required"/>
    </authentication>
  </security-domain>
```

Checklist de Instalación:

1. Revisar conectividad entre Frontend y Backend.
2. Chequear el acceso desde Frontend a PDI.
3. Certificados (En anexo 4 hay un diagrama explicativo de la ubicación de los certificados):
    a. SSL PDI
    b. Conector (Persona Juridica)
    c. Dominio HTTPS
    d. Red uy
4. Chequear que el backend este habilitado para realizar envío de correos.
5. Chequear reverse proxy.
6. DNS.
7. Validar que se accede a los servicios en PDI (consumo). (*)
8. Configuracion SSL en Backend.
9. HTTPS en Frontend.
10. Validar que se puede invocar servicios expuestos desde PDI

(*) Por más información como por ejemplo urls: Ver Manual de operaciones (Backoffice).

d. Diagrama de certificados


4 - SAML request firmado
5 - Token SAML firmado (redirect)
COESYS
Actor
1 - HTTPS (certificado host trazabilidad.pge.red.uy)
2 - Request
3 - SAML request firmado
Utiliza el certificado Persona Jurídica
6 - Request con token firmado por COESYS
Load Balancer
6
3
2
Utiliza el certificado de persona jurídica para enviar request en PDI
FRONTEND
APP01
Certificado SSL + Certificado Persona Jurìdica
EMISOR
(WS *)
VSHIELD
(8080 - http - ejb remoting)
VSHIELD
(8443 - HTTPS)
PDI
HTTP
HTTP
HTTPS
HTTPS
APP02
Certificado SSL + Certificado CA PDI
APP03
Certificado SSL + Certificado CA PDI
BACKEND