Consorci de Serveis Universitaris de Catalunya

Guia del projecte d'Evidències Electròniques (eLogs)

19-01-2015

Gran Capità, 2 (Edifici Nexus) • 08034 Barcelona • 93 205 6464 • www.csuc.cat NIF Q-5856253-I

Control de canvis

Data i versió	Descripció
19-01-15 v1	• Versió original

Sumari

1. Introducció

L'objectiu del present document es presentar en detall el funcionament de la plataforma d'evidències electròniques i d'explicar les característiques que té implementades la plataforma.

Requisits de la guia:

- Accés a la plataforma eLogs com administrador
- Programari SOAP UI.
- Projecte d'integració SOAP per a generar i descarregar Affidàvits.

1.2. Glossari

A continuació s'exposen una sèrie de termes que son usats en el següent document i que pot ser interessant conèixer, per entendre'l amb més facilitat:

- **Affidàvit** Segons la RAE un Affidàvit es defineix com:

  "Documento legal que sirve como testimonio o declaración jurada ante un tribunal, o como garantía o aval en otros casos"

  Per tant, a eviLogStack! un Affidàvit es un document privat, firmat electrònicament i segellat en el temps, en el qual es van recopilant les evidències necessàries per a poder demostrar davant un tercer que una determinada transacció electrònica s'ha produït

- **Shipper** Els Shippers són els agents d'eviLogStack!. Son petits desenvolupaments de programari que s'instal·len en servidores específics on es capturen les evidències bé de fitxers de text o d'accés a base de dades. També sobre els Shippers es despleguen els serveis web de remissió d'evidències.

- **Site** La nostra organització.

2. Passos previs

2.1. Instal·lació del programari SOAP UI

http://www.soapui.org/SOAP-and-WSDL/reference/All-Pages.html

http://sourceforge.net/projects/soapui/files/

2.2. Descàrrega del projecte d'integració per a generar evidències, crear i descarregar Affidàvits.

Contactar amb el servei d'Administració Electrònica del CSUC

Correu electrònic: auc@csuc.cat

Telèfon: 935516202

2.3. Accés a la plataforma d'eLogs com Administrador

Contactar amb el responsable del servei d'Evidències Electròniques del CSUC:

Nom: Josep Alemany Araujo

Correu electrònic: josep.alemany@csuc.cat

Telèfon: 935516202

O bé amb el cap de servei d'Administració Electrònica del CSUC:

Nom: Albert Portugal Brugada

Correu electrònic: albert.portugal@csuc.cat

Telèfon: 932055133

2.4. Validar la connectivitat amb els serveis d'eLogs des de la vostra institució

Validar que teniu accés a les següents URL's:

Des de l'equip de l'operador que accedirà a la web:

- https://elog.csuc.cat/

Des de l'equip de l'operador que configurarà les crides als webservices:

- http://elog.csuc.cat/api/metadata
- http://elog-agent.csuc.cat:8100/soap12

Per accedir als serveis s'haurà d'habilitar la connexió amb els següents ports:

- Web: 443
- Webservices: 8100
- Syslog: 514

2.5. Manuals d'usuari i programari

- http://www.csuc.cat/ca/e-administracio/evidencies-electroniques/manuals-d-usuari

3. Funcionalitats del sistema

A continuació es descriuran les diferents funcionalitats que conté la plataforma. Ens centrarem en els casos d'ús més importants.

3.1 Incorporació d'evidències al sistema

Existeixen diferents orígens possibles d'on recopilar les evidències i emmagatzemar-les al nostre sistema. A continuació els enumerem:

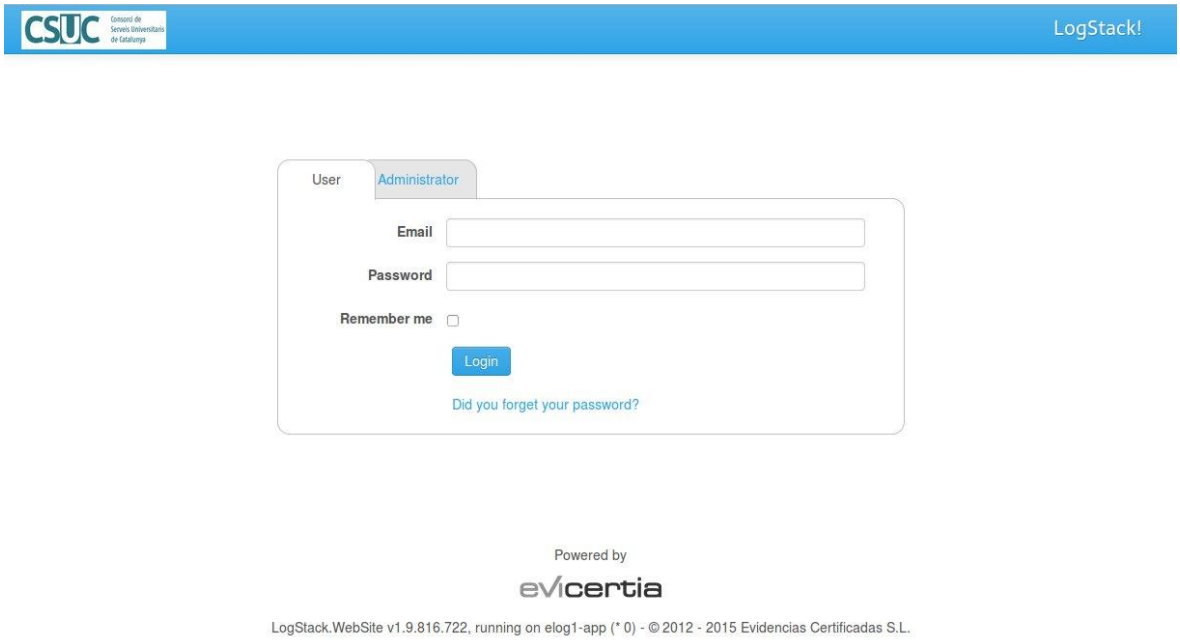
1. Webservices
2. Bases de dades
3. Retransmissió de logs

En el moment de crear i configurar el Shipper, indicarem quin serà l'origen de dades d'on extraurem les evidències.

3.2 Cerca d'evidències i generació d'Affidàvits

3.2.1 Autenticació a la plataforma

Per accedir al sistema ho haurem de fer amb les credencials prèviament assignades. Hi ha dos tipus d'accés, amb el rol d'usuari (que engloba a usuaris i administradors de Site) i amb el rol d'administrador.



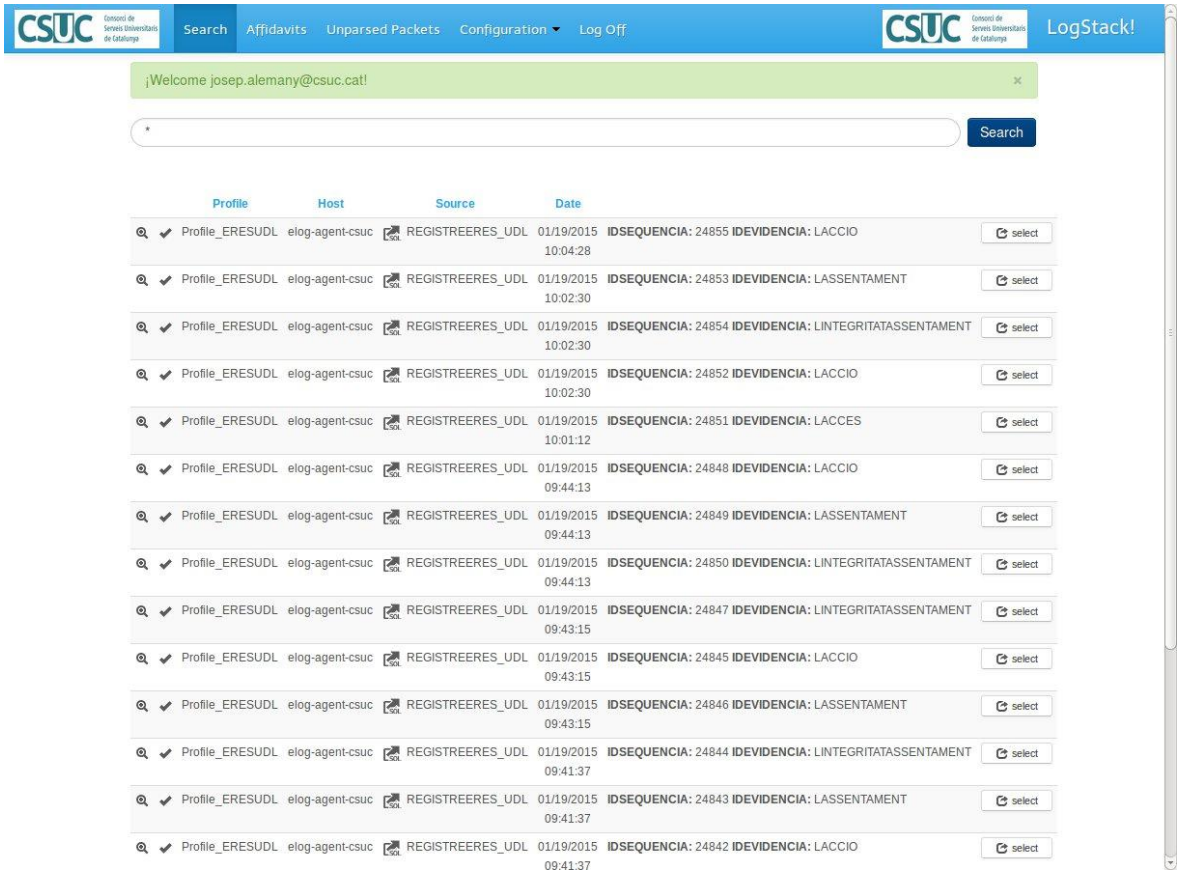
Imatge 1 – Autenticació

Altres utilitats d'aquesta pàgina d'accés al sistema serien les següents:

- Remember me, marcant aquesta opció, no és necessari autenticar-se cada cop que s'accedeix al sistema.
- Did you forget your password?, aquesta utilitat serveix per a enviar un correu electrònic amb la URL d'accés per a canviar el password.

3.2.2 Cercar evidències

La primera pantalla que es mostra per defecte és on surten totes les evidències recol·lectades pel nostre Shipper al nostre Site.



Imatge 2 – Cerca

Aquí podrem fer accions de filtratge amb expressions regulars de més o menys complexitat per seleccionar només aquelles que ens interessen. Es poden seleccionar aquelles evidències que es desitgi incorporar a l'Affidàvit polsant sobre el botó Select, que canviarà a Selected, i que a la vegada anirà canviant el número d'evidències que apareixen en el botó New affidavit (#), on # representa el número d'evidències.

Veiem algun exemple de com crear una expressió regular per aconseguir les evidències desitjades.

Las expressions regulars que es donen d'alta a la plataforma d'evidències electròniques sempre han de complir aquest format, on es poden donar d'alta tantes clau-valor como es cregui necessari.

```
(?<clave>[regex])
```

Per exemple, la següent expressió regular:

```
(?<date>[0-9][0-9][0-9][0-9]-[0-9][0-9]-[0-9][0-9]  [0-9][0-9]:[0-9][0-9]:[0-9][0-9]):(?<field1>[a-zA-Z0-9]*) (?<field2>[a-zA-Z0-9]*)
```

S'utilitza per descomposar els següents registres de línies de l'estil:

```
2013-10-25 15:58:58:primercamp20131025155858 segoncamp20131025155858
2013-10-25 15:58:59:primercamp20131025155859 segoncamp20131025155859
2013-10-25 15:59:00:primercamp20131025155900 segoncamp20131025155900
2013-10-25 15:59:01:primercamp20131025155901 segoncamp20131025155901
2013-10-25 15:59:02:primercamp20131025155902 segoncamp20131025155902
2013-10-25 15:59:03:primercamp20131025155903 segoncamp20131025155903
2013-10-25 15:59:04:primercamp20131025155904 segoncamp20131025155904
2013-10-25 15:59:05:primercamp20131025155905 segoncamp20131025155905
2013-10-25 15:59:06:primercamp20131025155906 segoncamp20131025155906
2013-10-25 15:59:07:primercamp20131025155907 segoncamp20131025155907
2013-10-25 15:59:08:primercamp20131025155908 segoncamp20131025155908
2013-10-25 15:59:09:primercamp20131025155909 segoncamp20131025155909
2013-10-25 15:59:10:primercamp20131025155910 segoncamp20131025155910
```

On, a més, s'identifiquen les claus <date>, <field1> i <field2>, que hauran de ser identificades prèviament en el perfil d'evidències desitjat.

Exemples

a) Fem un exemple sobre les evidències que tenim recol·lectades al sistema. Si per exemple volem cercar totes aquelles evidències que tenen el camp IDEVIDENCIA = LACCIO haurem de posar el següent al camp de cerca:

```
data.IDEVIDENCIA:LACCIO
```

El resultat serà el següent:

```
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     16:25:41
      IDSEQUENCIA: 25290 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     16:03:03
      IDSEQUENCIA: 25287 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:49:24
      IDSEQUENCIA: 25284 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:29:07
      IDSEQUENCIA: 25280 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:27:29
      IDSEQUENCIA: 25277 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:26:12
      IDSEQUENCIA: 25274 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:24:34
      IDSEQUENCIA: 25271 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:22:56
      IDSEQUENCIA: 25268 IDEVIDENCIA: LACCIO
```

```
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:21:27
       IDSEQUENCIA: 25265 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:20:19
       IDSEQUENCIA: 25262 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:19:01
       IDSEQUENCIA: 25259 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:17:43
       IDSEQUENCIA: 25256 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:16:05
       IDSEQUENCIA: 25253 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:14:07
       IDSEQUENCIA: 25250 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:12:19
       IDSEQUENCIA: 25247 IDEVIDENCIA: LACCIO
```

Si a més volem filtrar per un IDSEQUENCIA en concret posarem:

```
data.IDEVIDENCIA:LACCIO AND data.IDSEQUENCIA:25290
```

El resultat serà el següent:

```
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     16:25:41
       IDSEQUENCIA: 25290 IDEVIDENCIA: LACCIO
```

b) Un altre exemple més complert seria el següent:

Si volem filtrar la cerca per que ens mostri aquelles evidències d'un perfil determinat (ERES_UDL) i que s'hagin recollit entre les 15:30h i les 16:00h del dia 20 de Gener del 2015, aleshores farem el següent:

```
date:[2015-01-20T15:30:00 TO 2015-01-20T16:00:00] AND profile:Profile_ERESUDL
```

El resultat serà el següent:

```
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:49:24
       IDSEQUENCIA: 25285 IDEVIDENCIA: LASSENTAMENT
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:49:24
       IDSEQUENCIA: 25284 IDEVIDENCIA: LACCIO
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:49:24
       IDSEQUENCIA: 25286 IDEVIDENCIA: LINTEGRITATASSENTAMENT
Profile_ERESUDL     elog-agent-csuc     REGISTREERES_UDL    01/20/2015     15:48:16
       IDSEQUENCIA: 25283 IDEVIDENCIA: LACCES
```

c) Si el que volem és comprovar que un dels nostres agents ha recol.lectat una evidència en concret, podem cercar pel host i la dada desitjada:

```
host:elog-agent-csuc AND data.IDSEQUENCIA:6673
```

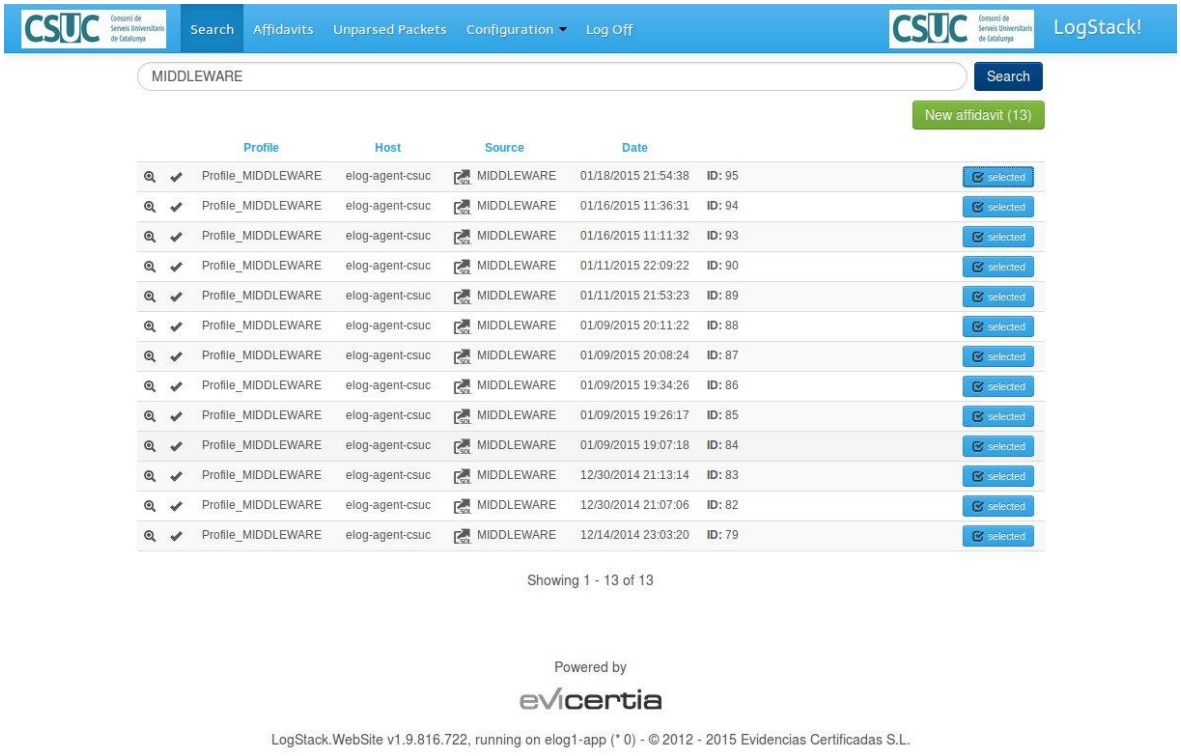
El resultat serà el següent:

```
Profile_REGISTREERES_CSUC elog-agent-csuc     REGISTREERES_CSUC   01/21/2015
15:35:43     IDSEQUENCIA: 6673 IDEVIDENCIA: LACCIO
```

NOTA: Veure la página
http://lucene.apache.org/core/2_9_4/queryparsersyntax.html

3.2.3 Generació d'Affidàvits

Per a la creació d'un Affidàvit haurem de seleccionar primer les evidències que vulguem que hi formin part. Per això és important realitzar una bona cerca prèviament de les mateixes.

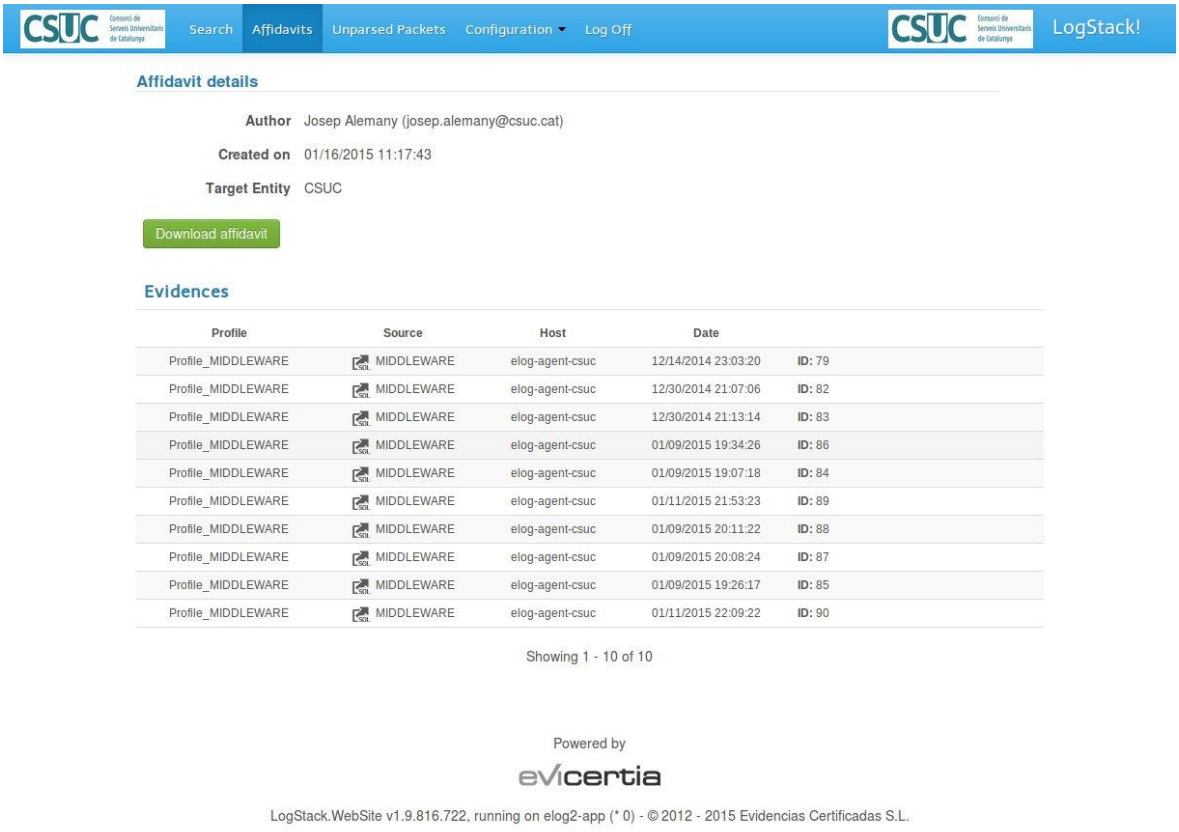


Imatge 3 – Creació d'un Affidàvit

Quan es polsa el botó New affidavit(#) s'accedeix a la pantalla d'Affidàvits, on és necessari omplir una sèrie de dades que serveixen per guardar l'Affidàvit. Les dades que s'han d'omplir les següents:

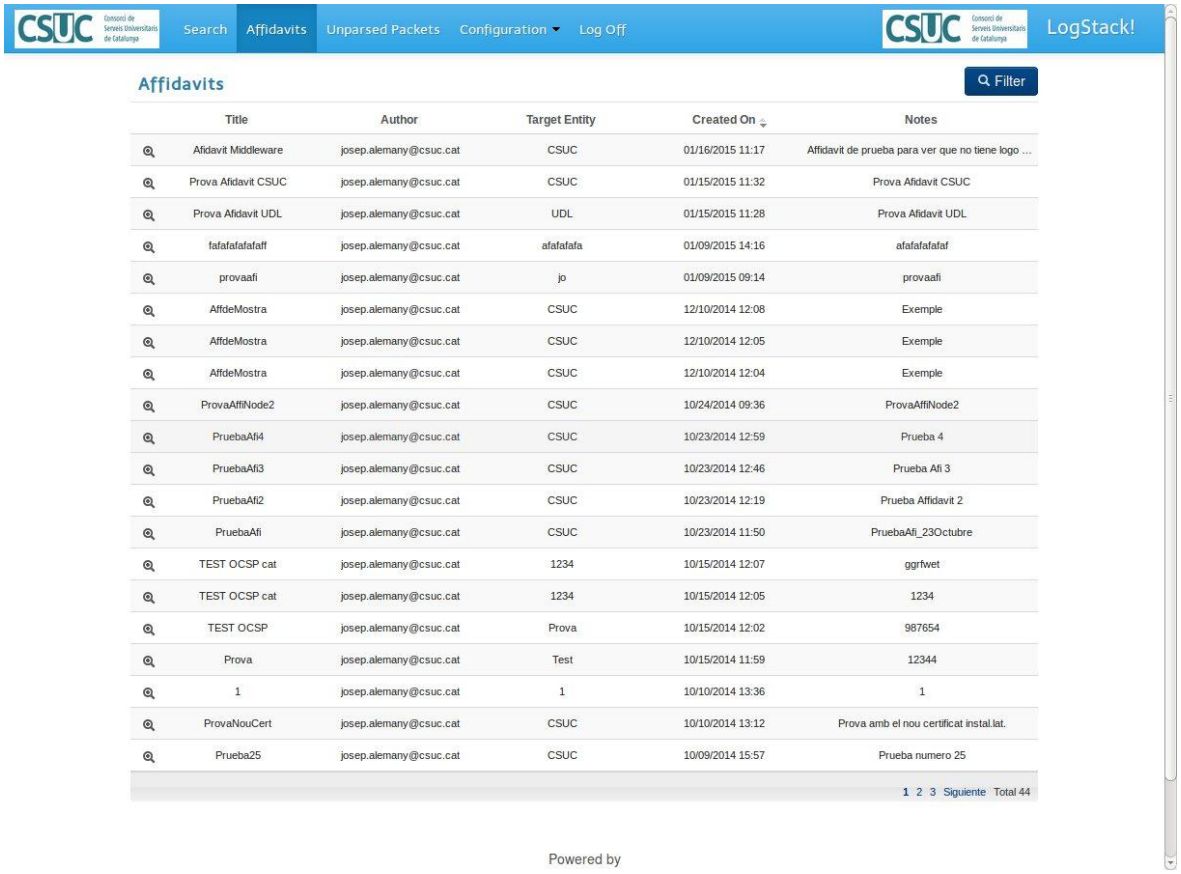
- Title, nom identificatiu que es vol donar a l'Affidàvit.
- Customer, entitat o persona que l'ha sol·licitat o per a la que es vol generar l'Affidàvit.
- Comments, camp lliure per a incloure comentaris o el que es consideri.

Al generar un nou Affidàvit, se'ns mostrarà un missatge de que s'està generant l'Affidàvit (aquest pot trigar uns minuts depenent de les evidències que s'hagin de processar). Finalment ens apareixerà un botó verd per iniciar la descàrrega de l'Affidàvit que s'acaba de generar:

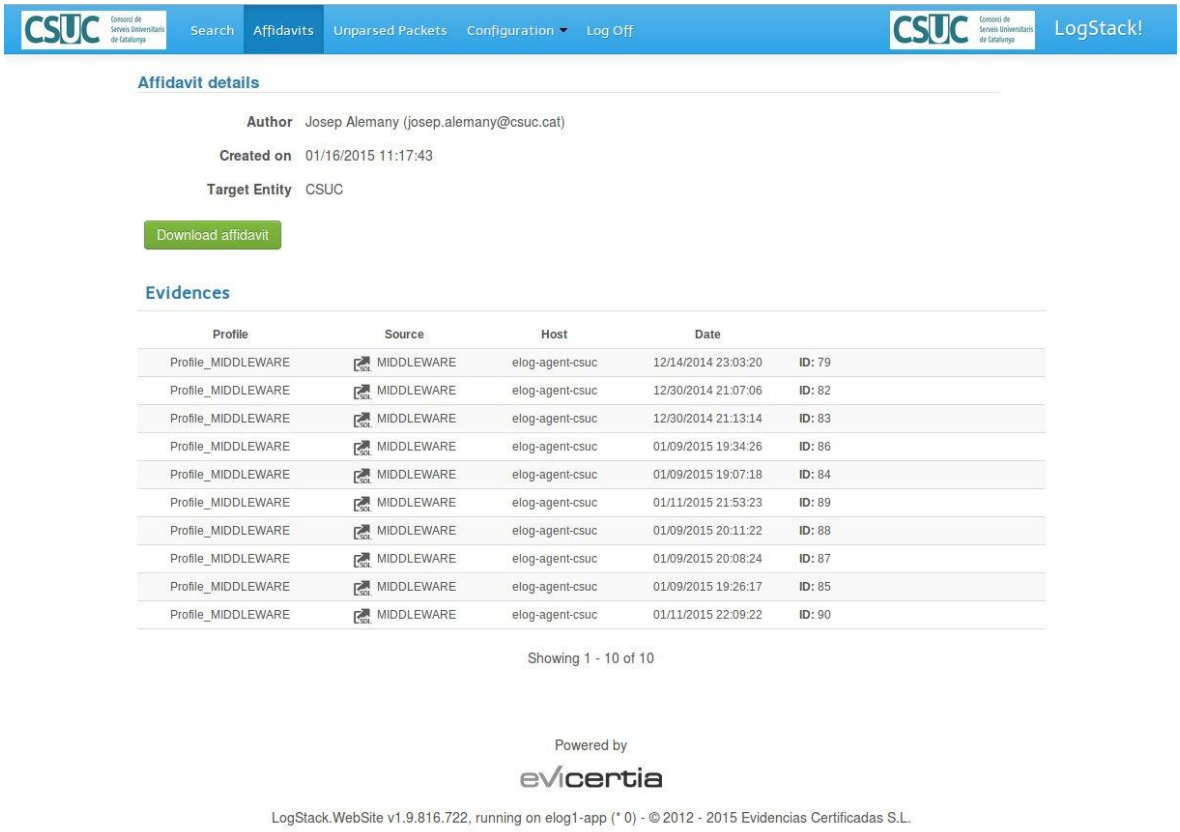


Imatge 4 – Descàrrega d'Affidàvit

De la mateixa manera es poden descarregar tots els Affidàvits que s'hagin generat prèviament des del menú Affidàvits i que pertanyin al nostre Site. Si es desitja visualitzar la informació d'un Affidàvit es polsa l'enllaç View i s'accedeix a la pantalla que conté les evidències i un accés l'Affidàvit firmat a través del botó Download affidavit.



Imatge 5 – Llistat d'Affidàvits



Imatge 6 – Descàrrega d'Affidàvits

3.3 Configuració d'usuaris de WebServices

La plataforma proporciona una capa de serveis web dual (SOAP + REST) i pot ser consumida mitjançant els següents estàndards:

- SOAP/1.1
- SOAP/1.2
- REST+XML
- REST+JSON
- REST+JSV
- REST+CSV

La plataforma té dos tipus de serveis web diferents:

- Serveis web desplegats al servidor web de la plataforma.
- Serveis web desplegats al propi Shipper.

3.3.1 Serveis web desplegats a la plataforma

Per al consum dels serveis web de la plataforma és necessari disposar d'un usuari actiu en l'esmentat servei ja que les peticions al sistema hauran d'emprar autenticació "HTTP Bàsica".

- Els serveis webs es poden trobar a la URL http://elog.csuc.cat/api/metadata

Per aquest motiu el supervisor del Site ha de configurar aquests comptes. Accedint a través del menú Configuració | WebServices s'accedeix a la gestió d'usuaris per als serveis web del Site.

Els serveis web pels que es necessita l'autenticació d'aquests usuaris son els següents:

- AffidavitDownload, servei web per la descàrrega d'un Affidàvit buscat pel seu identificador únic al sistema. El paràmetre a enviar via SOAP o REST és:
  - Id, identificador únic de l'Affidàvit dins de la plataforma.
- AffidavitRequest, servei web que permet generar Affidàvits a partir de la remissió d'identificadors d'evidències que ja estan donades d'alta a la plataforma. Els paràmetres a enviar via SOAP o REST son:
  - Evidences.GUID, un o varis GUID que identifiquen de manera unívoca evidències a la plataforma.
  - Title, text que apareixerà com a títol de l'Affidàvit.
  - TargetEntity, entitat que sol·licita l'Affidàvit.
  - Comments, comentaris a l'Affidàvit.
- Auth, servei web per a comprovar l'autenticació de la parella usuari/contrasenya d'un usuari ja creat anteriorment. Els paràmetres a enviar via SOAP o REST son:
  - UserName, usuari que es correspon amb el compte creat a la plataforma.
  - Password, contrasenya d'aquest usuari.
- EvidenceQuery, servei web que permet comprovar la informació de les evidències emmagatzemades al sistema. El paràmetre a enviar via SOAP o REST és:
  - Id, identificador únic de l'Affidàvit dins de la plataforma.

En aquest menú es pot donar d'alta, modificar i esborrar un usuari, també procedir al seu bloqueig si fos necessari, i a realitzar cerques sobre els mateixos.

3.3.2 Serveis web desplegats a l'agent

De la mateixa manera que pels serveis web desplegats al servidor, també serà necessari en aquest cas disposar d'un usuari actiu per consumir els serveis web desplegats a l'agent.

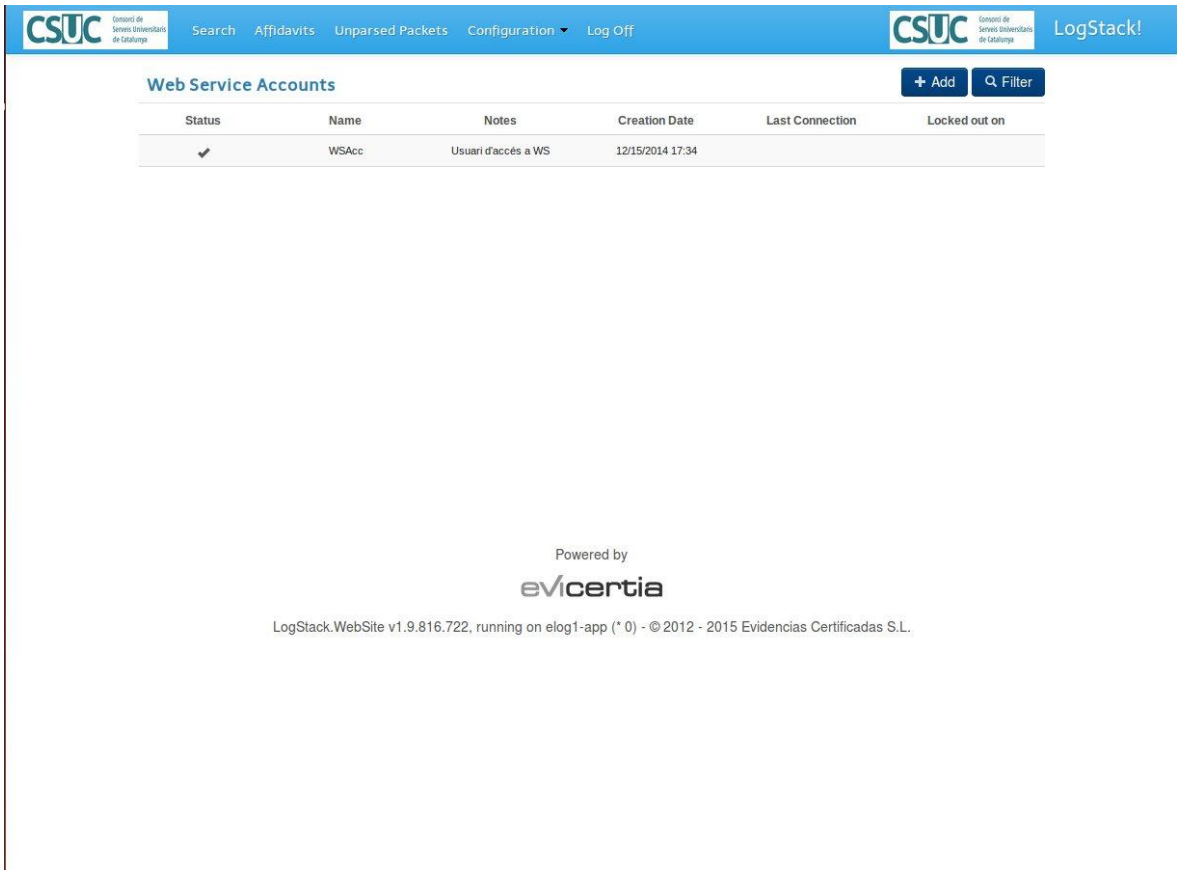
- Els serveis webs es poden trobar a la URL: http://elog-agent.csuc.cat/api/metadata

Accedint a través del menú Configuration | Shippers | WebService Accounts s'accedeix a la gestió d'usuaris per als serveis web de l'agent. Els usuaris es donen d'alta en aquest menú i posteriorment es desplegaran a l'agent mitjançant la sincronització que realitza l'agent contra el servidor cada minut.

Els serveis web pels que es necessita l'autenticació d'aquests usuaris son els següents:

- Auth, servei web per a comprovar l'autenticació de la parella usuari/contrasenya d'un usuari ja creat anteriorment. Els paràmetres a enviar via SOAP o REST son:
  - UserName, usuari que es correspon amb el compte creat a la plataforma.
  - Password, contrasenya d'aquest usuari.
- EvidenceSubmit, servei web que permet emetre evidències que seran processades per l'agent i posteriorment enviades al servidor. Els paràmetres a enviar via SOAP o REST son:
  - Profile: nom del perfil de l'evidència a aplicar a l'evidència.
  - MimeType: format de l'encapçalament de l'evidència.
  - Tags: etiqueta a aplicar a l'evidència. S'han d'incloure tants Strings com Tags a aplicar a l'evidència
    - String
  - Attributes: atributs a aplicar a l'evidència.
    - Key: clau de l'evidència.
    - Type: tipus.
    - Value: valor de la parella clau-valor.
  - Data: base64 de l'evidència a enviar a la plataforma.

En aquest menú es pot donar d'alta, modificar i esborrar un usuari, també procedir al seu bloqueig si fos necessari, i a realitzar cerques sobre els mateixos.



Imatge 7 – Webservice Accounts

3.4 Creació i configuració d'un agent (Shipper)

Accedint a través del menú Configuration | Shipper s'accedeix a la gestió dels agents que té desplegats el Site als seus sistemes. En aquest menú es poden donar d'alta, modificar i esborrar els agents, i realitzar cerques sobre els mateixos.

Imatge 8 – Llistat de Shippers donats d'alta al nostre Site

3.4.1 Què és un Shipper i com funcionen

Els Shippers son els agents que es despleguen als servidores de cara a facilitar la recol·lecció d'evidències el més a prop dels orígens d'informació.

L'alta d'un agent es correspon de dues parts ben diferenciades:

1. Al propi servidor on s'allotgi el Shipper, inicialment es crea un Shipper i es genera una parella de claus públic/privades, on la clau privada és la que es necessitarà per donar-la d'alta a la plataforma (veure punt 3.4.2) i que permetrà autenticar de manera unívoca l'agent dins de la plataforma.
2. A la plataforma es donarà d'alta la clau púbica de cada Shipper, d'aquesta manera els podrem autenticar.

Una vegada donat d'alta l'agent, cada minut es sol·licitarà una actualització de la configuració, per això invocarà el servei web ShipperConfigurationDownload que es

troba al servidor. L'autenticació es fa a través de la clau pública que s'ha donat prèviament d'alta al servidor.

3.4.2 Inicialitzant un Shipper en un agent virtual

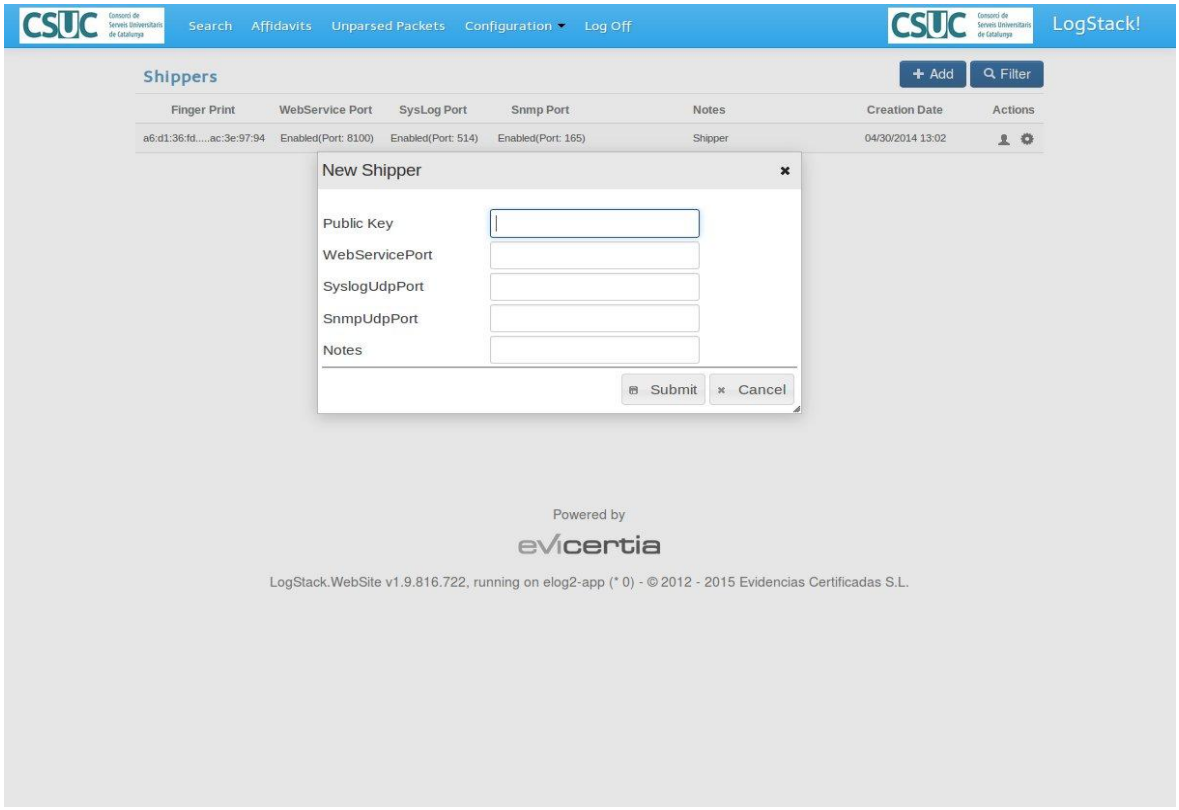
Es important destacar que la única operació que s'ha de fer sobre l'agent és la de la generació de les claus, ja que un cop generades les claus, la resta de configuracions de l'agent es poden realitzar via el portal web de la plataforma.

Per a inicialitzar un Shipper s'haurà d'executar la següent comanda al servidor virtual:

```
[root@shipper1 ~]# mono /opt/LogStack/Shipper/LogStack.Shipper.exe setup -server-address http://<ip>/api
Saving http://<ip>/api/metadata as server uri..
Generating RSA key pair..
Saving generated key pair with fingerprint: a0:8a:e4:04:ba:3c:96:a8:c8:61:92:42:dd:c5:b7:fe:0b:d6:d9:c3
```

3.4.3 Alta / modificació / baixa d'un Shipper

Entrem al portal web de la plataforma i accedim al menú Shipper. Per procedir a afegir el nou agent que acabem de inicialitzar al nostre servidor virtual hem de polsar el botó +ADD.



Imatge 9 – Creació d'un nou Shipper

Les dades que s'han de donar d'alta son:

- Public Key, és la clau pública generada durant el procés d'alta del Shipper. Per conèixer aquesta informació, ens haurem de connectar a la màquina virtual on tinguem desplegat l'agent i executar la següent comanda:

```
[root@shipper1 ~]# mono /opt/LogStack/Shipper/LogStack.Shipper.exe show-
pubkey
Public Key fingerprint:
62:42:20:b9:02:63:4e:1a:32:00:3b:25:fa:06:2e:f1:74:48:eb:7c
Public Key (in PKCS#8/PEM format):
MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDJZscZ9BD1gyR3T4UD71+eT2FR1nZqNMToCo
sYhxe+Ikbs3Yu//y7KEoPtSJU3PeE1O8pKmN+tsReYvUNHfXXg3mNkz/ABaus5chyHzzQoYdh8
Oc6tri8KNJDVILiIMO0pNqbvG86Z3pKAsqEo5MzWdo+Pou3H6vE6Z/HDk+2XjwIBEQ==
```

  La informació a copiar és la part corresponent a la Public Key.
- WebService Port, port on el servei web estarà configurat. És important destacar que si existeixen tallafocs als servidor dels agents, aquests han d'obrir aquest port al protocol TCP per que de manera externa es puguin consumir els serveis web desplegats.
- Syslog Port, port on es configurarà el servei syslog remot.
- SNMP Port, port que es configurarà per escoltar la recol·lecció de traces SNMP.
- Notes, informació addicional, no obligatòria, referent a l'agent que es vulgui incloure.

Per a modificar o eliminar un agent, només haurem de seleccionar-lo i apareixeran els botons d'editar i esborrar al menú superior. De la mateixa manera que en el cas d'esborrar un agent, es sol·licitarà confirmació abans de procedir a l'esborrat del mateix.

Una vegada donat d'alta un agent, s'han de configurar els orígens de dades (*sources)* i els comptes de webservices *(webservices accounts)*(**vist al punt 3.3.2**).

Com es veu a la següent imatge, hi ha dos enllaços que ens porten a:

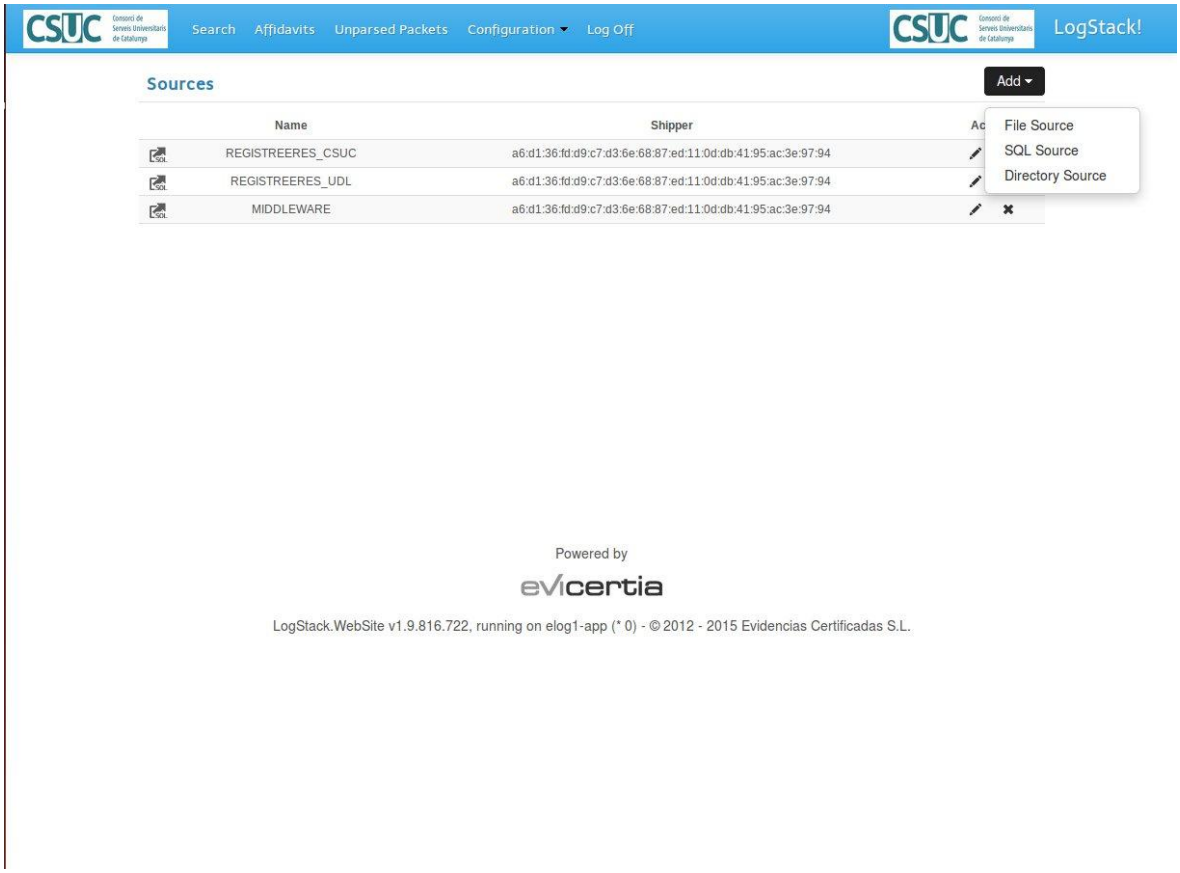
- Pantalla de configuració de WebService accounts.
- Pantalla de gestió dels orígens de dades del Site, on es pot realitzar la gestió dels diferents orígens.

Imatge 10 – Accions sobre el Shipper

Ens centrarem ara en el segon cas.

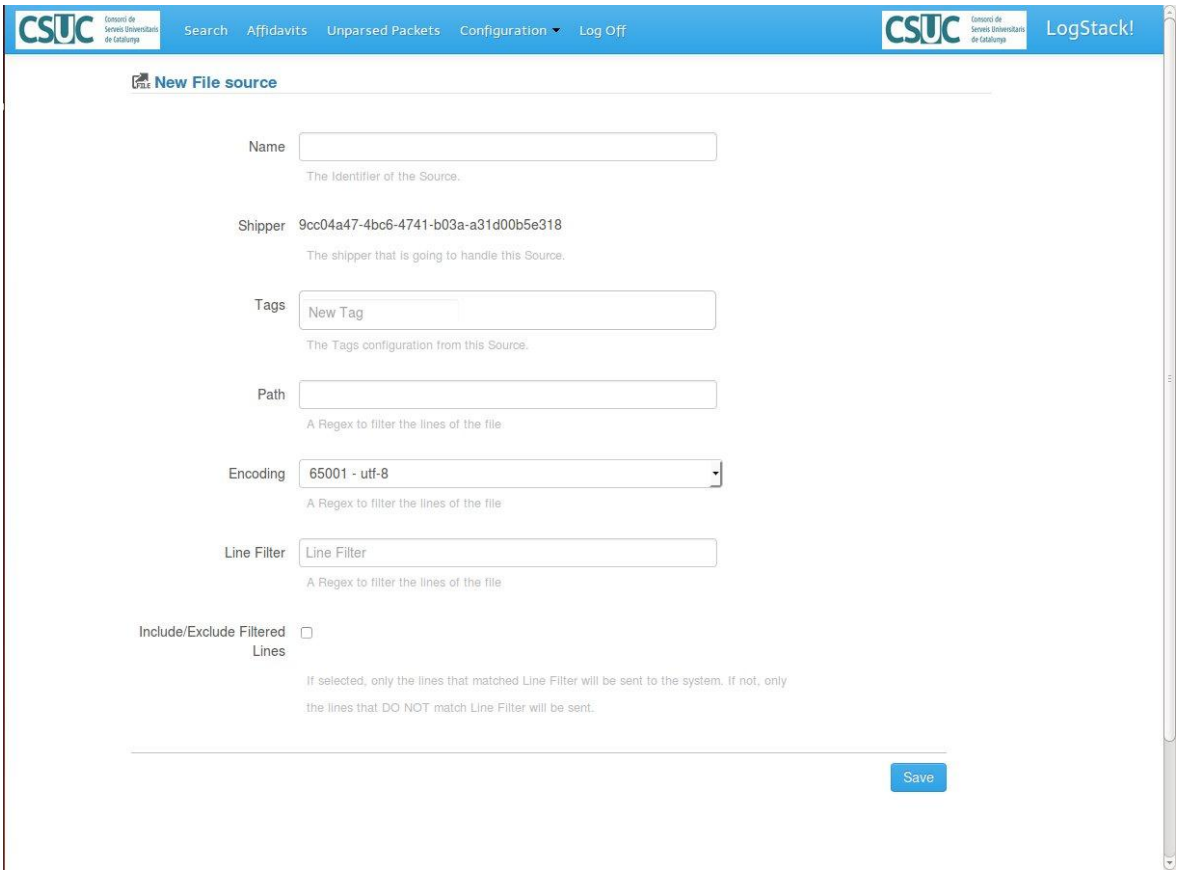
Un cop a dins de la configuració dels sources, per crear un nou origen de dades s'ha de polsar el botor Add+, que ens mostrarà el tipus d'orígens de dades que es poden donar d'alta:

- File Source, origen de dades per a fitxers.
- SQL Source, origen de dades per a bases de dades.
- Directory Source, origen de dades per a fitxers XML depositats en un directori.



Imatge 11 – Orígens de dades de l'agent

Seleccionant qualsevol, ens portarà a la pantalla de creació d'origen de dades en funció de l'origen seleccionat.



Imatge 12 – Pantalla d'alta d'un origen de dades del tipus fitxer a l'agent

A continuació s'indiquen els camps de cadascun dels orígens de dades, començant pels comuns a tots, i especificant a continuació els individuals.

- Name, nom que s'assignarà a l'origen de dades.
- Shipper, camp que permet identificar l'agent que tindrà aquest origen de dades.
- Custody Period, període de custodia que es vol guardar l'evidència.
- Tags, etiquetes que s'afegiran a totes les evidències que reculli aquest agent d'aquest origen de dades. Aquestes etiquetes seran molt importants, ja que més tard seran necessàries per realitzar les cerques i per poder processar-les a les regles de parsejat d'evidències.
- <CampsEspecífics> de File Source,
    - Path, ruta del fitxer sobre el que es guardarà l'evidència.
    - Encoding, codificació d'aquest fitxer (normalment serà UTF-8, però pot variar).
    - Line Filter, permet incloure una expressió regular per poder-la utilitzar com a filtre.

- Include/Exclude Filtered Lines, si es marca i s'ha especificat una Line Filter, només que coincideixi amb l'expressió regular s'enviarà al servidor. Si no es marca, només s'enviaran al servidor el que no coincideixi amb l'expressió regular.

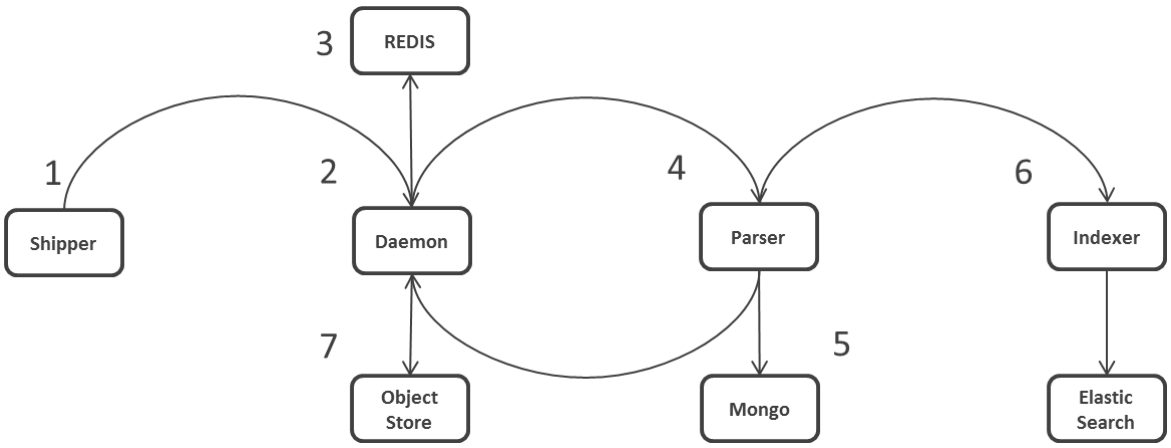
- <CampsEspecífics> de Database Source,
  - Connection String, cadena de connexió a la base de dades. Aquesta cadena de connexió dependrà de cada tipus de gestor de base de dades. Per exemple, una cadena de una connexió amb Postgresql: Server=localhost;Port=5432;UserID=postgres;Password=;Database=preLogStackShipper1;MaxPoolSize=300;enlist=False;Timeout=90;CommandTimeout=90
  - Table Name, nom de la taula o vista sobre la que es capturarà l'evidència.
  - Cursor column, columna que conté l'identificador únic de la tabla.
  - Driver, camp desplegable amb els drivers implementats al servei.
- <CampEspecífic> de Directory Source,
  - Path, ruta del directori on es guardaran les evidències.

En quant al Syslog i a l'SNMP, una vegada configurats els ports del Syslog i d'SNMP, l'agent ja estarà habilitat per a poder escoltar en aquests ports i recopilar la informació que s'enviï. Aquesta informació s'envia mitjançant el protocol UDP, per tant, només serà necessari configurar perfils d'evidències i parsers per a tractar la informació.

Finalment, la forma de modificar o esborrar orígens de dades ja definits seria seleccionant el que es vol modificar o esborrar i procedir com qualsevol altre acció de modificació o esborrat que hem vist fins ara.

Annex I. Flux de les evidències

A continuació a mode de resum, s'explicarà de forma breu el flux generat per una evidència des de que es recol·lecta, es firma i finalment es custodia a la plataforma d'evidències electròniques.



Imatge 13 – Flux d'una evidència

A continuació s'especifiquen els passos recollits al diagrama anterior:

1. Les evidències son recol·lectades pel Shipper. La configuració del Shipper la fa el supervisor a través de la web de la plataforma. A la web es donen d'alta els orígens de dades que son els encarregats de indicar al Shipper on poden recol·lectar les evidències. Al Shipper es generen dos tipus de paquets diferents:
   a. DataPacket, son els paquets que contenen l'evidència a processar.
   b. SignaturePacket, son els paquets que contenen la informació que garantitza la integritat dels DataPacket enviats des del Shipper fins al servidor d'evidències electròniques. Un SignaturePacket pot contenir informació de varis DataPacket.
2. Quan les evidències estan llestes al Shipper, s'envíen al RabbitMQ(1) i d'allà són recollides pel Daemon(2).
3. El Daemon el primer que fa es posar totes les evidències en quarantena fins que tingui tots els DataPackets i SignaturePacket associats a una sèrie d'evidències. Aquests paquets en quarantena s'emmagatzemen a Redis(3).
4. Quan es poden processar totes les evidències en quarantena s'envien al RabbitMQ per a que siguin recollits pel Parser(4).
5. El Parser recull totes les evidències i comença a processar-la en funció de les regles donades d'alta al sistema. En cas de no poder procedir a parsejar la informació, l'evidència s'envia a Mongo(5) per que es pugui visualitzar a la web de la plataforma dins del menú "Unparsed Packet(6)".

6. Si el Parser processa correctament les evidències, les envia al RabbitMQ per a que l'Indexer(7) les reculli i procedeixi a la indexació de les mateixes. Si tot funciona correctament es guarda la informació de l'evidència a l'Elastic Search(8).
7. En paral·lel al pas anterior, l'evidència també s'envia al Daemon que s'encarregarà de guardar-la i les dades relatives a la integritat de les mateixes a l'ObjectStore(9). És en aquesta part del procés on es sol·licitarà el segell de temps.

(1) RabbitMQ - Software de gestió de cues.
(2) Daemon - Dimoni encarregat de processar els missatges del Shipper (via RabbitMQ).
(3) Redis - Motor de base de dades en memòria, basat en l'emmagatzemament de taules de hashos (clau-valor).
(4) Parser - Es comunica amb el Daemon per poder processar els missatges i enviar-los al Indexer.
(5) Mongo - Gestor de base de dades orientat a documents.
(6) Unparsed Packet - Menú on es visualitza la llista de paquets no parsejats.
(7) Indexer - Recull els events enviats pel Shipper, els "normalitza" i els inserta a ElasticSearch.
(8) Elastic Search - Servidor de cerques basat en Lucene.
(9) Object Store - Emmagatzema de forma segura les evidències originals capturades i els Affidàvits generats**.**