D4Science Infrastructure - Task #3480

Enable SSL on ldap-liferay.d4science.org

Apr 15, 2016 08:46 PM - Andrea Dell'Amico

Status:	Closed	**Start date:**	Apr 15, 2016
Priority:	Urgent	**Due date:**	
Assignee:	_InfraScience Systems Engineer	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	SSL everywhere		
Infrastructure:	Development, Production		

Description

The service is still using non encrypted connections.

When all the services will have switched to the encrypted connection, the non ssl port will be closed.

Related issues:

Blocked by D4Science Infrastructure - Task #3481: Add ldap.d4science.org as C...	**Closed**	**Apr 15, 2016**

History

#1 - Apr 15, 2016 08:48 PM - Andrea Dell'Amico

- Description updated

@massimiliano.assante@isti.cnr.it let me know when we can make the configuration change. A ldap restart is needed. It's a matter of seconds if all goes well.

#2 - Apr 15, 2016 08:49 PM - Andrea Dell'Amico

- Blocked by Task #3481: Add ldap.d4science.org as CNAME of ldap-liferay.d4science.org added

#3 - Apr 19, 2016 11:11 AM - Massimiliano Assante

- Status changed from New to In Progress

I'm available to discuss about this. If I understand correctly we need to change the service endpoint configuration pointing to it.
In order to perform this change, each production portal service endpoint must be updated (see

```
<Endpoint EntryName="LDAPServer">ldap://ldap-liferay.d4science.org</Endpoint>)
```

and each production portal must be restarted.

I should also check if the java method which connects to this ldap instance has no problem with SLL. Should we give this a try in ldap-liferay dev instance? Is that working on SSL yet?

#4 - Apr 19, 2016 11:17 AM - Andrea Dell'Amico

- Infrastructure Development added

- Yes, the development ldap server is under ssl already.
- I also added two aliases, because ldap-liferay is now misleading: ldap-d.d4science.org is an alias for ldap-liferay-d.d4science.org and ldap.d4science.org is an alias for ldap-liferay.d4science.org. Note that the certificate for the dev instance does not covers the alias yet, I'll add it in some minutes.
- If the java standard CA list contains the parent CA for the letsencrypt certificates it should have no problems. I only checked with non java clients though, and the Oracle JRE/JDK use their private CA certs list.
- I can activate the ssl endpoint and maintain the non ssl one until all the services will be switched.

#5 - Apr 19, 2016 11:24 AM - Andrea Dell'Amico

Andrea Dell'Amico wrote:

> - I also added two aliases, because ldap-liferay is now misleading: ldap-d.d4science.org is an alias for ldap-liferay-d.d4science.org and ldap.d4science.org is an alias for ldap-liferay.d4science.org. Note that the certificate for the dev instance does not covers the alias yet, I'll add it in some minutes.

I stand corrected. The automatic procedure correctly updated the certificate last night and correctly reloaded the openldap server. So you can already test against the dev ldap service using ldaps://ldap-d.d4science.org (the SSL port is the 636 one if you need to set it explicitly).

#6 - Apr 19, 2016 12:20 PM - Massimiliano Assante

tried in dev, have the following exception

```
javax.naming.CommunicationException: simple bind failed: ldap-d.d4science.org:636 [Root exception is javax.net
.ssl.SSLHandshakeException: java.security.cert.CertificateException: Invalid Server Certificate: server certif
icate could not be verified, and the CA certificate is missing from the certificate chain. raw error: sun.secu
rity.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilde
rException: unable to find valid certification path to requested target]
```

#7 - Apr 19, 2016 12:40 PM - Andrea Dell'Amico

The CA used by letsencrypt is not known to the JRE, but the problem lies here:

```
-Djavax.net.ssl.trustStore=/etc/ssl/cacerts_isti
```

We used a personalized trust store because the ISTI pop/imap servers use an invalid CA and the pop/imap sessions failed for that reason. There was a ticket about it in the old issue tracker.
I'm going to generate a new java keyring adding the CA chain used by letsencrypt. It will substitute the one currently used.

#8 - Apr 19, 2016 05:51 PM - Massimiliano Assante

- % Done changed from 0 to 50

now in dev.d4science.org it worked

```
2016-04-19 15:49:21,900 INFO  ldapexport.LDAPSync [http-9090-1,<init>:52] %[PORTAL] 716481 [http-9090-1] INFO
 org.gcube.portal.ldapexport.LDAPSync  - Starting LDAPSync over ldaps://ldap-d.d4science.org
2016-04-19 15:49:24,971 DEBUG ldapexport.LDAPSync [pool-11-thread-1,exportSingleUsers:216] %[PORTAL] 719552 [p
ool-11-thread-1] DEBUG org.gcube.portal.ldapexport.LDAPSync  - LDAP Users Sync cycle done
2016-04-19 15:49:24,972 INFO  ldapexport.LDAPSync [pool-11-thread-1,exportSingleUsers:218] %[PORTAL] 719553 [p
ool-11-thread-1] INFO  org.gcube.portal.ldapexport.LDAPSync  - LDAP Users Sync Completed OK!
```

#9 - Apr 19, 2016 05:53 PM - Andrea Dell'Amico

- % Done changed from 50 to 30

I'm installing the new keyring on all the portal hosts.
It should not be needed on any other servers with an up to date jdk.

#10 - Apr 19, 2016 06:45 PM - Andrea Dell'Amico

The new keyring has been installed on:

```
descramble.d4science.org
egip.d4science.org
i-marine.d4science.org
preprod.d4science.org
services.d4science.org

infra-gateway.d4science.org

dev.d4science.org
dev2.d4science.org
dev3.d4science.org
```

To actually use it, the following option needs to be passed to the java VM:

```
-Djavax.net.ssl.trustStore=/etc/ssl/cacerts_isti
```

#11 - Apr 19, 2016 06:50 PM - Massimiliano Assante

also on preprod.d4science.org please

#12 - Apr 19, 2016 06:54 PM - Andrea Dell'Amico

It's already there, it's listed together with the production hosts.

#13 - Apr 20, 2016 02:13 PM - Andrea Dell'Amico

- % Done changed from 30 to 90

The ldap server is now running with ssl enabled.
This redmine instance is already configured to bind on the ssl port.

#14 - Apr 21, 2016 01:10 PM - Andrea Dell'Amico

The sobigdata.eu drupal instance has started using ssl, FIY.

#15 - Apr 26, 2016 07:05 PM - Massimiliano Assante

- % Done changed from 90 to 100

LDAP configuration changed for production portal successfully, now contacting ldaps://ldap-liferay.d4science.org

#16 - Apr 26, 2016 07:09 PM - Andrea Dell'Amico

Thanks. I plan to close the plain text ldap port next Monday.

#17 - May 02, 2016 02:30 PM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

Done.

#18 - May 05, 2016 01:59 PM - Andrea Dell'Amico

- Status changed from Feedback to Closed