



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR INFORMATICS
ISA Integrated Collaborative Platform

European Commission

Solr installation procedure

Date: 25/07/2013
Version: 1.000
Authors: everis
Revised by:
Approved by:
Public:
Reference Number:

TABLE OF CONTENTS

1.	OVERVIEW OF THE SOLR MACHINE	2
2.	DIRECTORIES AND FILESYSTEMS	2
3.	APACHE SETUP	3
4.	TOMCAT SETUP	3
5.	DRUPAL CONFIGURATION	3
6.	MAKE SOLR DATA PUBLICLY AVAILABLE.....	3

1. OVERVIEW OF THE SOLR MACHINE

You could install a solr in a standard LAMP machine. And as Solr is a Java-based service, a Tomcat instance has to be enabled.

Joinup uses a virtual machine with 4 CPUs and 16 GB of RAM.

2. DIRECTORIES AND FILESYSTEMS

The /environment/app/webroot/icp_home/solr directory will contain everything related to Solr. For the moment, we only need a single Solr instance, so we will setup a "Solr home" in the "joinup_acceptance" subdirectory:

```
# Download Solr
wget http://apache.crihan.fr/dist/lucene/solr/3.1.0/apache-solr-3.1.0.tgz
# Extract the instance example
tar xzv --strip-components=2 -f apache-solr-3.1.0.tgz apache-solr-
3.1.0/example/solr
# and the Solr war
tar xzv -O -f apache-solr-3.1.0.tgz apache-solr-3.1.0/dist/apache-solr-3.1.0.war
> solr/apache-solr-3.1.0.war

# Download the "apachesolr" Drupal module
wget http://ftp.drupal.org/files/projects/apachesolr-6.x-1.5.tar.gz
# extract solrconfig.xml and schema.xml and insert them into the Solr home conf
directory
tar xzv -O -f apachesolr-6.x-1.5.tar.gz apachesolr/solrconfig.xml >
solr/conf/solrconfig.xml
tar xzv -O -f apachesolr-6.x-1.5.tar.gz apachesolr/schema.xml >
solr/conf/schema.xml

# We'll need a data directory to store indexes generated by Solr and a lib
directory if we want to use plugins in the future.
mkdir -p solr/{lib,data}

# rename our solr home directory
mv solr joinup_acceptance
```

Transfer the joinup_acceptance directory into solr:/environment/app/webroot/icp_home/solr/. Ensure at least the "data" directory is writable by the webrun user.

3. APACHE SETUP

Add this snippet to the Apache configuration to "protect" the Solr home:

```
# Solr configuration
<Directory "/environment/app/webroot/icp_home/solr">
    # ensure no one can reach the Solr home through Apache
    Order Deny,Allow
    Deny From All
</Directory>
```

4. TOMCAT SETUP

We now need to deploy the Solr application above Tomcat. We will add a new context to the Catalina configuration: `/local/tomcat/5.5.29/conf/Catalina/localhost/joinup-solr.xml`. It should contain:

```
<?xml version="1.0" encoding="utf-8"?>
<Context
docBase="/environment/app/webroot/icp_home/solr/joinup_acceptance/apache-
solr.war" debug="1" crossContext="true">
    <Environment
        name="solr/home"
        type="java.lang.String"
value="/environment/app/webroot/icp_home/solr/joinup_acceptance"
override="true"/>
</Context>
```

- In case we use Solr plugins, add `/environment/app/webroot/icp_home/solr/joinup_acceptance/lib/*.jar` at the end of the `common.loader` property in `/local/tomcat/5.5.29/conf/catalina.properties`
- Restart the Tomcat server
- `solr.eu.int:8080/joinup-solr` should display "Welcome to Solr!"

5. DRUPAL CONFIGURATION

In the `settings.php` configuration file of the Drupal application:

1. ensure the following is added:

```
// Solr-dedicated, environment-specific configuration
// we use the http://solr.eu.int:8080/joinup-solr Solr instance
$config['apachesolr_host'] = 'XXX.XXX.X.XXX'; // solr.eu.int
$config['apachesolr_port'] = '8080';
$config['apachesolr_path'] = '/joinup-solr';
// It appears the Solr client may require a JRE...
$config['apachesolr_attachments_java'] =
'/local/tomcat/jdk1.6.0_21/jre/bin/java';
```

2. In case of proxy: ensure `$config['proxy_exceptions']` contains 'solr.eu.int'; otherwise, the Drupal application would try to reach the Solr instance through its proxy, which would not work.

6. MAKE SOLR DATA PUBLICLY AVAILABLE

In our case, Joinup relies on the use of reverse-proxy as security system. That implies, that to make data publicly available, it's required a security mapping of <http://solr.eu.int:8080/joinup-solr/select>.

This way, read-only requests can be made from the Internet, while other handlers (`/update`, `/admin`, ...) can only be reached from within your domain.

A good practice is to implement a white list of servers authorized to contact these handlers to limit the risk of an internal attack.