

Instalación GeoServer en producción

Acerca de

Documento publicado bajo licencia Creative Commons reconocimiento compartir-igual (CC-by-sa). Consultar autoría y fecha en la siguiente tabla. Contribuciones bienvenidas.

Versión	Fecha	Autor(es)	Cambios
1.0	27/02/2014	Oscar Fonts	Compilación a partir de documentación de CTBB, FAO, Roses e i3dat. Actualizadas versiones: OpenJDK 1.7, Tomcat 7, GeoServer 2.5 beta. Testeado en Ubuntu 12.04 server x64.

Prerrequisitos

Hardware y SO

- Sistema Operativo: Recomendado Ubuntu 12.04 Server 64 bits
- CPU: 2 cores mínimo, 4 cores recomendado
- RAM: 2 GB mínimo, 4 GB recomendado
- Disco: Según cantidad de datos a publicar (contar con la caché de teselas)

Configuración inicial de la máquina

Configurar conexión y nombre de la máquina:

```
ifconfig eth0 <public_ip> <mask>
route add default gw <gateway>

echo "<nombre>" > /etc/hostname
hostname -F /etc/hostname
```

/etc/hosts debería contener:

```
127.0.0.1    localhost.localdomain  localhost
<public_ip> <nombre>.example.com  <nombre>
```

Zona horaria:

```
dpkg-reconfigure tzdata
```

Actualizar paquetes:

```
apt-get update
apt-get upgrade
```

Algunas utilidades básicas:

```
apt-get install vim locate
updatedb
```

Instalar y configurar firewall (iptables):

```
apt-get install iptables

iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p tcp -m multiport --destination-ports 22,80,5432 -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP

iptables-save > /etc/iptables.rules
```

/etc/network/interfaces debería cargar las reglas de iptables al arrancar:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
    pre-up iptables-restore < /etc/iptables.rules
```

Instalar fail2ban:

```
apt-get install fail2ban
service fail2ban restart
```

Crear usuarios SUDOers:

```
adduser <name>
adduser <name> sudo
```

Bloquear login de ROOT vía SSH. Cambiar esta línea /etc/ssh/sshd_config:

```
PermitRootLogin no
```

Reiniciar servicio ssh:

```
service ssh reload
```

Evitar el error 'too many files open'...

Añadir esta línea a /etc/sysctl.conf:

```
fs.file-max = 5120
```

Añadir esta línea a /etc/security/limits.conf

```
* - nofile 5120
```

Tras reiniciar la máquina, comprobar límite con:

```
ulimit -n
```

Instalar fuentes de Microsoft:

```
apt-get install ttf-mscorefonts-installer
```

Instalar OpenJDK 7 y Tomcat 7:

```
apt-get install openjdk-7-jdk
apt-get install tomcat7
```

Añadir JAI y JAI-ImageIO nativos:

```
cd /usr/lib/jvm/java-7-openjdk-amd64
wget http://download.java.net/media/jai/builds/release/1_1_3/jai-1_1_3-lib-linux-amd64-jdk.bin
sh jai-1_1_3-lib-linux-amd64-jdk.bin

wget http://download.java.net/media/jai-imageio/builds/release/1.1/jai_imageio-1_1-lib-linux-amd64-jdk.bin
export _POSIX2_VERSION=199209
sh jai_imageio-1_1-lib-linux-amd64-jdk.bin

service tomcat7 restart
```

Instalar GDAL (1.10):

```
apt-get install python-software-properties
add-apt-repository ppa:ubuntugis/ubuntugis-unstable
apt-get update
apt-get install gdal-bin
```

PostGIS

Instalar PostgreSQL (9.1) y PostGIS (2.0):

```
apt-get install postgresql
apt-get install postgresql-9.1-postgis-2.0
```

Habilitar acceso local. En /etc/postgresql/9.1/main/pg_hba.conf:

#	TYPE	DATABASE	USER	ADDRESS	METHOD
local	all		postgres		ident
local	all		all		md5
host	all		all	127.0.0.1/32	md5

Y en /etc/postgresql/9.1/main/postgresql.conf, descomentar:

```
listen_addresses = 'localhost'
```

Reiniciar para aplicar cambios:

```
service postgresql restart
```

Para acceder a la consola SQL:

```
sudo -u postgres psql
```

Crear un nuevo "usuario":

```
CREATE USER usuario LOGIN PASSWORD '-----' NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
```

Crear una nueva BDD "geodatos" cuyo propietario sea "usuario":

```
sudo -u postgres createdb -O usuario geodatos
```

Habilitar capacidades "geo" en la base de datos:

```
sudo -u postgres psql -d geodatos -c "CREATE EXTENSION postgis;"
```

PgAdmin III

Para instalar la versión más reciente de pgAdmin en ubuntu, crear el fichero /etc/apt/sources.list.d/pgdg.list con este contenido:

```
deb http://apt.postgresql.org/pub/repos/apt/ precise-pgdg main
```

Y luego, activar el nuevo repo e instalar pgadmin3 (versión 1.18):

```
wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add -
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install pgadmin3
```

Acceso remoto mediante túnel SSH

Para el acceso remoto a una BDD, se recomienda usar última versión de pgAdmin (1.18), que tiene la opción de acceder mediante un túnel SSH. Al crear una nueva conexión:

1. Pestaña propiedades:

- Nombre: <nombre>
- Host: localhost
- Port: 5432
- Maintenance DB: <base de datos>
- Username: <usuario>
- Password: (da igual, lo va a preguntar siempre)

2. Pestaña "SSH Tunnel":

- Use SSH tunneling: Checked
- Tunnel host: nombre de la máquina
- Username: usuario de la máquina
- Authentication: Usar password. No hace falta escribirlo, lo preguntará cada vez.

Acceso remoto abriendo puerto

En caso de tener que abrir directamente un puerto (opción menos segura):

1. En /etc/postgresql/9.1/main/postgresql.conf:

```
listen_addresses = '*' # O mejor, una lista de IPs, si son fijas.
```

2. En `/etc/postgresql/9.1/main/pg_hba.conf`, añadir una línea específica de acceso para una combinación de IP, BDD y usuario determinados (a ser posible, no usar comodines o "all" para el acceso remoto).

Configuración de SSL (https) en tomcat 7

1. Autogenerar certificado (para pruebas; usar certificado real en producción):

```
cd /var/lib/tomcat7
keytool -genkey -alias admin -keypass adminpass -keystore certificate.bin -storepass adminpass
chown tomcat7:tomcat7 certificate.bin
```

2. Añadir (descomentar) el conector SSL en `/var/lib/tomcat7/conf/server.xml`, asignarle el puerto 443, y redirigir el servicio HTTP de 8080 al puerto 443:

```
<Connector port="8080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  URIEncoding="UTF-8"
  redirectPort="443" />

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="certificate.bin" keystorePass="adminpass" />
```

3. Permitir a Tomcat usar puertos estándar, por debajo de 1024. Editar `/etc/default/tomcat7` y editar la directiva AUTHBIND:

```
AUTHBIND=yes
```

4. Forzar el uso de SSL para todas las aplicaciones, inhabilitando el puerto 8080 convencional. Añadir este contenido a `/var/lib/tomcat7/conf/web.xml`:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Protected Context</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

5. Reiniciar tomcat:

```
service tomcat7 restart
```

GeoServer

Instalación base

GeoServer (latest, unstable):

```
cd /var/lib/tomcat7/webapps/  
wget http://sourceforge.net/projects/geoserver/files/GeoServer/2.5-beta/geoserver-2.5-beta-war.zip  
apt-get install unzip  
unzip geoserver-2.5-beta-war.zip  
rm -rf target/ *.txt geoserver-2.5-beta-war.zip
```

Entorno JVM

Mover el GEOSERVER_DATA_DIR fuera de los binarios:

```
mv /var/lib/tomcat7/webapps/geoserver/data /var/lib/geoserver_data  
mkdir /var/lib/geowebcache_data  
chown tomcat7:tomcat7 /var/lib/geowebcache_data
```

Editar el fichero /etc/default/tomcat7 y añadir al final las rutas a Java, los datos, la caché, y parámetros de optimización:

```
JAVA_HOME=/usr/lib/jvm/java-7-openjdk-amd64  
  
GEOSERVER_DATA_DIR=/var/lib/geoserver_data  
GEOWEBCACHE_CACHE_DIR=/tileCache  
  
JAVA_OPTS="-server -Djava.awt.headless=true -Xms1560m -Xmx1560m -XX:PermSize=384m -XX:MaxPermSize=512m -XX:+UseConcMarkSweepGC -XX:NewSize=48m -DGEOSERVER_DATA_DIR=$GEOSERVER_DATA_DIR -DGEOWEBCACHE_CACHE_DIR=$GEOWEBCACHE_CACHE_DIR"
```

Reiniciar tomcat:

```
service tomcat7 restart
```

Comprobación entorno

Entrar a:

```
http://<maquina>:8080/geoserver/web/
```

En "server status", comprobar que:

- El Data directory apunta a /var/lib/geoserver_data
- La JVM es la instalada (OpenJDK 1.7 64 bits)
- Native JAI y Native JAI ImageIO están a "true"

Seguridad

Seguir las notificaciones de seguridad que aparecen en la página principal de GeoServer:

- Cambiar password de "admin".
- Cambiar el master password.

Configuración Web

Bajo "About & Status":

- Editar la información de contacto. Esto aparecerá en los servicios WMS públicos: dejar a "Claudius Ptolomaeus" es indecente.

Bajo "Data":

- Borrar todos los espacios de trabajo (workspaces) existentes.
- Borrar todos los estilos existentes (dirá que hay 4 que no los puede borrar, esto es correcto).

Bajo "Services":

- WCS: Deshabilitar si no va a usarse.
- WFS: Cambiar el nivel de servicio a "Básico" (a menos que queramos permitir la edición remota de datos vectoriales).
- WMS: En "Limited SRS list", poner sólo las proyecciones que deseamos anunciar en nuestro servicio WMS. Esto reduce el tamaño del GetCapabilities. Por ejemplo: **23029, 23030, 23031, 25829, 25830, 25831, 4230, 4258, 4326, 3857, 900913**.

Bajo "Settings":

- Global: Cambiar el nivel de logging a PRODUCTION_LOGGING.

Bajo "Tile Caching":

- Caching Defaults: Activar los formatos "image/png8" para capas vectoriales, "image/jpeg" para capas ráster, y ambas para los grupos de capas.
- Disk Quota: Habilitar la cuota de disco. Tamaño máximo algo por debajo de la capacidad que tenga la unidad de Tile Caché.

Cambio de datum con malla NTv2

Descargar el fichero de malla de:

<https://github.com/oscarfonts/gt-datumshift/blob/master/icc-tests/src/test/resources/org/geotools/referencing/factory/gridshift/100800401.gsb>

Copiar el fichero de malla en user_projections:

```
cp 100800401.gsb /var/lib/geoserver_data/user_projections/
chown tomcat7:tomcat7 100800401.gsb
```

Forzar que se use también para la proyección Google Earth. Crear un fichero en user_projections llamado epsg_operations.properties, con el siguiente contenido:

```
4230,4258=PARAM_MT["NTv2", PARAMETER["Latitude and longitude difference file", "100800401.gsb"]]
4230,4326=PARAM_MT["NTv2", PARAMETER["Latitude and longitude difference file", "100800401.gsb"]]
```

Cambiar el owner:

```
chown tomcat7:tomcat7 epsg_operations.properties
```

Reiniciar GeoServer:

```
service tomcat7 restart
```

Comprobar que se utiliza la malla para reproyectar entre "EPSG:4230" y "EPSG:4258", y entre "EPSG:4230" y "EPSG:4326".

Esto se puede comprobar en la web de GeoServer, bajo "Demos" => Reprojection Console.

Añadir soporte para formatos ECW y SID

1. Instalar la extensión "GDAL" correspondiente a la versión de GeoServer:
<http://sourceforge.net/projects/geoserver/files/GeoServer%20Extensions/>

```
cd /var/lib/tomcat7/webapps/geoserver/WEB-INF/lib/
wget http://sourceforge.net/projects/geoserver/files/GeoServer%20Extensions/2.5-beta/geoserver-2.5-beta-gdal-plugin.zip
unzip geoserver-2.5-beta-gdal-plugin.zip
rm *.txt *.TXT *.zip
chown tomcat7:tomcat7 *.jar
```

2. Instalar las definiciones CRS (gdal_data):

```
cd /var/lib/geoserver_data
mkdir gdal
cd gdal
wget http://demo.geo-solutions.it/share/github/imageio-ext/releases/1.1.X/1.1.8/gdal/gdal-data.zip
unzip gdal-data.zip
```

3. Instalar las librerías nativas de GDAL:

```
mkdir lib
cd lib
wget http://demo.geo-solutions.it/share/github/imageio-ext/releases/1.1.X/1.1.8/gdal/linux/gdal192-Ubuntu12-gcc4.6.3-x86_64.tar.gz
tar -xvf gdal192-Ubuntu12-gcc4.6.3-x86_64.tar.gz
```

4. Añadir variables de entorno, a /etc/default/tomcat7:

```
GDAL_DATA=$GEOSERVER_DATA_DIR/gdal/gdal-data
LD_LIBRARY_PATH=$GEOSERVER_DATA_DIR/gdal/lib
```

5. Cambiar permisos y reiniciar tomcat:

```
chown -R tomcat7:tomcat7 /var/lib/geoserver_data/
service tomcat7 restart
```

Se listarán los nuevos formatos al crear un almacén de datos raster.

Warning

Utilizar ECW en un servidor sin comprar una licencia a ERDAS es ilegal.

Para usar el formato ECW en un servidor de mapas, es necesario leer y aceptar esto:
<http://demo.geo-solutions.it/share/github/imageio-ext/releases/1.1.X/1.1.7/native/gdal/linux/ECWEULA.txt>

Extensiones Oficiales

CSS. Simbolizar más fácil que con SLD:

```
http://sourceforge.net/projects/geoserver/files/GeoServer%20Extensions/2.5-beta/geoserver-2.5-beta-css-plugin.zip
```

Importer. Crear capas de un conjunto de tablas PostGIS o de ficheros ráster sin tener que ir una a una:

```
http://sourceforge.net/projects/geoserver/files/GeoServer%20Extensions/2.5-beta/geoserver-2.5-beta-importer-plugin.zip
```

Control Flow. Evita sobresaturar el servidor:

```
http://sourceforge.net/projects/geoserver/files/GeoServer%20Extensions/2.5-beta/geoserver-2.5-beta-control-flow-plugin.zip  
http://docs.geoserver.org/latest/en/user/extensions/controlflow/index.html
```

LibJPEG Turbo. Acelera salida en JPEG:

```
http://sourceforge.net/projects/libjpeg-turbo/files/1.3.0/libjpeg-turbo-official\_1.3.0\_amd64.deb  
dpkg -i libjpeg-turbo-official_1.3.0_amd64.deb  
Añadir /opt/libjpeg-turbo/lib64 a LD_LIBRARY_PATH en /etc/default/tomcat7.  
http://sourceforge.net/projects/geoserver/files/GeoServer%20Extensions/2.5-beta/geoserver-2.5-beta-libjpeg-turbo-plugin.zip
```


Extensiones "community"

Cómo compilarlas

No están mantenidas oficialmente, y no forman parte del "build" oficial. Hay que compilarlos desde las fuentes:

```
git clone git@github.com:geoserver/geoserver.git
cd geoserver
# git tag -l
git checkout -b tags/2.5-beta
cd src/community
mvn clean install -PcommunityRelease,proxy -DskipTests
mvn assembly:single
# Proxy jar generated in: proxy/target/gs-proxy-2.5-beta.jar
# Printing extension generated in: target/release/geoserver-2.5-beta-printing-plugin.zip
```

Cómo instalarlas

Proxy: wget en WEB-INF/lib:

```
https://dl.dropboxusercontent.com/u/2368219/geoserver/gs-proxy-2.5-beta.jar
```

Printing: wget y unzip en WEB-INF/lib:

```
https://dl.dropboxusercontent.com/u/2368219/geoserver/geoserver-2.1-printing-plugin-parxejat.zip
```

Cómo configurarlas

Ejemplo de configuración para la extensión de printing (copiar en /var/lib/geoserver_data/printing/):

<https://dl.dropboxusercontent.com/u/2368219/geoserver/config.yaml>

Esquema de teselado del ICC

La Tile Caché del ICC sigue un esquema de teselado particular, distinto al utilizado habitualmente por la mayoría de aplicaciones de web mapping. Por tanto, debe definirse en GeoServer este esquema particular de teselado:

- Sistema de coordenadas: EPSG:23031
- Límites:
 - Min X: 258000
 - Min Y: 4485000
 - Máx X: 536000
 - Máx Y: 4752000
- Ancho y alto tesela: 256 x 256 px.

Nombre *

ICC_gridset

Descripción

Gridset compatible amb els nivells de zoom de la tilecaché del ICC (23031)

Sistema de coordenadas de referencia

EPSG:23031

Buscar...

EPSG:ED50 / UTM zone 31N...

Unidades: m

Metros por unidad: 1.0

Límites del conjunto de mallas

Min X

Min Y

Máx X

Máx Y

258,000

4,485,000

536,000

4,752,000

Calcular a partir de la extensión máxima del CRS

Ancho de la tesela en píxeles *

256

Alto de la tesela en píxeles *

256

Tile Matrix Set

Define las cuadrículas a partir de:

Resolutions

Scale denominators

Nivel	Tamaño de píxel	Escala	Nombre	Teselas
0	1,100	1: 3,928,571.428571429	Catalunya en 1 tile	1 x 1
1	550	1: 1,964,285.714285714	Catalunya en 2x2 tiles	2 x 2
2	275	1: 982,142.8571428573	Catalunya en 4x4 tiles	4 x 4
3	100	1: 357,142.8571428571	Escala 1:1 000 000	11 x 11
4	50	1: 178,571.4285714285	Escala 1:500 000	22 x 21
5	25	1: 89,285.71428571429	Escala 1:250 000	44 x 42
6	10	1: 35,714.28571428572	Escala 1:100 000	109 x 105
7	5	1: 17,857.14285714286	Escala 1:50 000	218 x 209
8	2	1: 7,142.857142857143	Escala 1:20 000	543 x 522
9	1	1: 3,571.428571428571	Escala 1:10 000	1,086 x 1,043
10	0.5	1: 1,785.714285714285	Escala 1:5 000	2,172 x 2,086
11	0.25	1: 892.8571428571429	Escala 1:2 500	4,344 x 4,172
12	0.1	1: 357.14285714285717	Escala 1:1 000	10,860 x 10,430

Matriz de teselas, defiida a partir de resolución en m/px:

Nivel	Tamaño del píxel	Nombre
0	1100	Catalunya en 1 tile
1	550	Catalunya en 2x2 tiles
2	275	Catalunya en 4x4 tiles
3	100	Escala 1:1 000 000
4	50	Escala 1:500 000
5	25	Escala 1:250 000
6	10	Escala 1:100 000
7	5	Escala 1:50 000
8	2	Escala 1:20 000
9	1	Escala 1:10 000
10	0.5	Escala 1:5 0000
11	0.25	Escala 1:2 500
12	0.1	Escala 1:1 000