

Instalación de Wormbase: Guía Completa

1) PREREQUISITOS

Esta sección describe los requisitos para la instalación.

1.1) Requerimientos de Hardware

WormBase corre en sistemas Unix o Linux. Un sistema relativamente rápido con una memoria generosa es altamente recomendado. El hardware mínimo sugerido es:

900 Mhz Pentium III o mejor

4 gigabytes RAM

4 gigabytes Swap

20 gigabytes de espacio libre en disco duro

Cada base de datos ocupa aproximadamente 5GB de disco duro, y usted necesitará al menos el doble para poder organizar y descomprimir las nuevas versiones de las bases de datos. Además, guarde otro GB más para ser usado por la base de datos BLAST.

WormBase actualmente está en una transición entre un sistema basado en AceDB y uno que corre en lo más alto de la base de datos relacional MySQL. Por esta razón, requiere ambos, AceDB y MySQL, para poder estar bien instalado. La capa de middleware para AceDB es AcePerl, y la capa de middleware para MySQL es el Bio::DB::Módulo GFF, que viene con el paquete BioPerl.

1.2) Requerimientos de Software

Necesitará los siguientes paquetes de software:

acedb version 4.8j o más nueva: <http://www.acedb.org/>

Perl version 5.6.1 o más nueva: <http://www.perl.org/>

Los siguientes módulos Perl, todos ellos disponibles en <http://www.cpan.org>, con las versiones listadas abajo o más nuevas:

1.2.1) Módulos requeridos

- Ace 1.87
- Bio::Das 0.20
- CGI 3.01
- CGI::Cache 1.40
- Cache::FileCache 0.09
- DBD::mysql 2.1026
- DBI 1.35
- Digest::MD5 2.24
- GD 1.19 (2.x recomendado)
- IO::Scalar 2.104
- IO::String 1.02
- LWP 5.69
- Net::FTP 2.67
- Statistics::OLS 0.07
- Storable 2.06
- Text::Shellwords 1.00

1.2.2) Modulos opcionales

- GD::SVG 0.25
- SVG 2.28
- XML::Dom 1.34
- XML::Parser 2.31
- XML::Twig 3.09
- XML::Writer 0.4

(Particularmente anotese el numero de la version del CGI.pm; Los bugs en las versiones más viejas de CGI.pm pueden causarle confusiones con WormBase.)

Si los modulos XML opcionales estan instalados, el navegador de genomas será capaz de arrojar las versiones GAME y BSML de las anotaciones de secuencia. Si los modulos GD::SVG y SVG estan instalados, el navegador de genomas será capaz de producir salidas en formato SVG.

1.2.3) Otras aplicaciones

- Apache 1.3.26 o más nuevo: <http://www.apache.org/>
- Mod_Perl 1.27 o más nuevo: <http://perl.apache.org/>
- Expat 1.95.1 o más nuevo: <http://expat.sourceforge.net/>
- El software de la Web de WormBase, que debe coincidir con la version de la data: <ftp://www.wormbase.org/pub/wormbase/software> o vía CVS
- El paquete Generic Genome Browser, version 1.61 o más nuevo: <http://www.gmod.org/>
- El paquete BioPerl, version 1.40 o más nuevo: <http://www.bioperl.org/>
- Wublast 2.0 o más nuevo (requerido para las paginas de busqueda BLAST): <http://blast.wustl.edu/>
- BLAT 2.7 o más nuevo (requerido para las paginas de busqueda BLAST): <http://www.soe.ucsc.edu/~kent/>
- La base de datos de MySQL, version 3.23.39 o más nuevo: <http://www.mysql.com/>
- Versión modificada de e-PCR (requerido para la pagina de busqueda e-PCR)
Localizada en el directorio "e-PCR" en la distribución Wormbase. Solo debe hacer cd hasta el directorio y tipear "make" y "make install". El archivo README-Wormbase describe los cambios que le fueron realizados a la distribución e-PCR.

2) PREPARANDO DIRECTORIOS Y USUARIOS

WormBase usa distintas cuentas de usuario para entablar permisos a los directorios y al servidor. Usted necesitará crear a estos usuarios y a varios directorios preliminares.

Cuentas de usuario y de grupos

Estos usuarios no deberían tener una contraseña para conectarse. Son creados solo para establecer privilegios.

Grupo aceDB

Este es el grupo que tendrá privilegios de escritura en el arbol de directorios de acedb. Los administradores Acedb deberían ser agregados a este grupo.

Usuario aceDB

Este es el usuario con el que el servidor acedb empezará. Debería ser un miembro del grupo aceDB.

Grupo Wormbase

Este es un grupo que tendrá privilegios de escritura en el árbol de directorios de Wormbase. Los administradores y autores de Wormbase deberían ser agregado a este grupo.

Creando un nuevo usuario y grupo varia entre las opciones de Unix. En la mayoría de sistemas Linux, los comandos siguientes crearán los nuevos grupos. Usted debería agregar el privilegio sudo para ejecutar estos comandos.

```
# /usr/sbin/groupadd acedb
# /usr/sbin/groupadd wormbase
```

y esto creará un nuevo usuario acedb:

```
# /usr/sbin/useradd -g acedb -d /usr/local/acedb acedb
```

Este comando también agrega al nuevo usuario aceDB al grupo aceDB.

Nota: El directorio home del usuario aceDB fue escrito como /usr/local/acedb, un directorio que será creado en el próximo paso.

Directorios

Cree los siguientes directorios:

```
/usr/local/acedb, owner=acedb group=acedb,mode=drwxrwsr-x
# mkdir /usr/local/acedb
# chown acedb /usr/local/acedb
# chgrp acedb /usr/local/acedb
# chmod 2775 /usr/local/acedb
```

```
/usr/local/wormbase, owner=root group=wormbase mode=drwxrwsr-x
# mkdir /usr/local/wormbase
# chown root /usr/local/wormbase
# chgrp wormbase /usr/local/wormbase
# chmod 2775 /usr/local/wormbase
```

```
/usr/local/wormbase/logs, owner=root group=wormbase mode=drwxrwsr-x
# mkdir /usr/local/wormbase/logs
# chown root /usr/local/wormbase/logs
# chgrp wormbase /usr/local/wormbase/logs
# chmod 2775 /usr/local/wormbase/logs
```

```
~ftp/pub/wormbase, owner=root group=wormbase mode=drwxrwsr-x
# mkdir ~ftp/pub/wormbase
# chown root ~ftp/pub/wormbase
# chgrp wormbase ~ftp/pub/wormbase
# chmod 2775 ~ftp/pub/wormbase
```

```
/usr/local/wublast, owner=root group=wormbase mode=drwxrwsr-x
# mkdir /usr/local/wublast
# chown root /usr/local/wublast
# chgrp wormbase /usr/local/wublast
# chmod 2775 /usr/local/wublast
```

Usted puede ignorar este paso sin problemas si no planeas incorporar la página de búsqueda BLAST.

El bit "s" en los permisos de grupo para esos directorios aseguran que los nuevos directorios y archivos creados dentro de ellos serán poseídos por el mismo grupo que el del directorio raíz. Esto permite a los grupos de administradores tener acceso a lectura/escritura de los archivos del proyecto. Para que esto funcione, sin embargo, la máscara de usuarios por defecto de estos individuos debe ser puesta en 002 cuando se conectan.

Este debería ser un buen momento para agregarse a usted mismo a los grupos aceDB y Wormbase.

```
# usermod -M acedb,wormbase [su_nombre_de_cuenta]
```

Usted podría necesitar reconectarse para que los cambios surtan efecto. Use los comandos de grupo para chequear de cuales grupos es miembro:

```
% groups
```

3) INSTALANDO LOS ARCHIVOS WORMBASE

Tiene dos opciones al instalar los archivos WormBase, por CVS o desde un archivo tarball. Ambos metodos son presentados. WormBase es un recurso dinamico; la version CVS le permitirá permanecer en el borde de la sangría. Sin embargo, no se garantiza que los scripts en CVS sean funcionales. Por esta razon, es recomendado usar una instalación tarball.

3.1) Instalando desde una publicacion tarball

Busque y descomprima el archivo wormbase-site-X.XX.tar.gz dentro de algun lugar seguro.

```
% cd ~/build # Un directorio constructor temporal en su home por ejemplo
% curl -O ftp://ftp.wormbase.org/software/wormbase-site-current.tar.gz
% gunzip -cd wormbase-site-current.tar.gz | tar xvf -
```

Ahora mueva sus contenidos a /usr/local/wormbase:

```
% cd wormbase-site*
# cp -r * /usr/local/wormbase/.
```

3.2) Instalando vía CVS

Al usar CVS de forma anonima le permitirá actualizar el software WormBase facilmente.

Cambie la variable de entorno CVSROOT: tcsh syntax: %setenv CVSROOT
:pserver:anonymous@gorgonzola.cshl.org:/usr/local/cvs

Sintaxis Bash:

```
%export CVSROOT=:pserver:anonymous@gorgonzola.cshl.org:/usr/local/cvs
```

```
% cd /usr/local/wormbase
% cvs -d:pserver:anonymous@gorgonzola.cshl.org:/usr/local/cvs \
co wormbase-site
% mv wormbase-site/* .
```

Y ahora, del unico directorio que necesita preocuparse es wspec, el cual contiene el esqueleto de los archivos de configuracion y la contraseña AceDB que necesitará para levantar y correr AceDB.

4) INSTALANDO ACEDB

Usted debe tener un servidor socket AceDB funcionando. Para mejores resultados el servidor debería estar corriendo sobre la misma maquina que el sitio web de WormBase. Este proceso es explicado en detalle porque es la parte más dificil al instalar un sitio WormBase. Puede instalar AceDB desde un paquete binario o un archivo fuente.

4.1.1) Instalando AceDB desde un paquete binario

Los siguientes comandos extraerán la ultima version de AceDB dentro de un directorio constructor temporario.

```
% cd ~/build
% mkdir acedb ; cd acedb
```

```

% curl -O http://www.acedb.org/Software/Downloads/SUPPORTED/ACEDB-
STATIC_serverLINUX.4_9t.tar.gz
% curl -O http://www.acedb.org/Software/Downloads/SUPPORTED/ACEDB-
STATIC_binaryLINUX.4_9t.tar.gz
% gunzip -c ACEDB-* | tar xvf -
  Si esto no funciona, trate de extraer cada objeto independientemente
  % zcat /usr/local/TGZ/ACEDB-STATIC_binaryLINUX.4_9t.tar.gz | tar xf -
  % zcat /usr/local/TGZ/ACEDB-STATIC_serverLINUX.4_9t.tar.gz | tar xf -
% mv ACEDB-* ~/mirror/src/. # Coloque el fuente si lo prefiere

```

Ahora copie los binarios extraidos en el directorio bin acedb, alterando los permisos según corresponda. #
 mkdir ~/acedb/bin # mv *~/acedb/bin/. # chown root ~acedb/bin/* # chgrp root ~acedb/bin/*

4.1.2) Instalando AceDB desde un archivo fuente

Descargue la version más reciente del Acedb, el cual es ACEDB-source.4_9m.tar.gz en este momento desde el sitio <http://www.acedb.org>.

Nota: Usted no debería extraer el archivo fuente tar.gz, ya que será descomprimido y desempaquetado automáticamente por el script INSTALL (vera los detalles mas adelante). También descargue los siguientes archivos:

```

NOTE
README (lista resumida/descripcion de archivos)
INSTALL (un script ksh, se instala una vez)

```

Ponga todos los archivos .tar.gz que necesites y luego INSTALL dentro de este directorio ~acedb/. El script instalará los paquetes en su directorio de trabajo actual.

```

# sudo chmod u+x INSTALL
# ./INSTALL

```

Nota: Permita que los archivos .tar.gz sean leibles para el grupo acedb.

En la terminal, se leerá: ...directory permissions OK... Files will be owned by: "nchen" Files will be installed in: /usr/local/acedb

Esto instalará el paquete como un subdirectorio del directorio actual. Si tal directorio existe usted tendrá la opción de no instalar ese paquete o abortar la instalacion completamente.

IMPORTANTE: NO LO INSTALE COMO ROOT: eso crearía un agujero de seguridad.

4.2) Construyendo Acedb con todo el sistema de copias del software GNU

```

# cd source
# setenv ACEDB_MACHINE LINUX_4
# make all

```

Puede encontrar todos los archivos binarios en el directorio bin.LINUX_4.

Cree el directorio /usr/local/acedb/bin (conocido como ~acedb/bin mas adelante, siempre que haya creado un usuario aceDB). Copie los siguientes archivos a este directorio:

```

saceserver
saceclient
sgifaceserver
tace
giface
xace
makeUserPasswd

```

Asegurese de que estos archivos son ejecutables y poseidos por root:

```

# chown root ~acedb/bin/

```

chgrp root ~acedb/bin/*

4.3) Instalando una base de datos preliminar y testeando Acedb

Necesitará una base de datos para testear si acedb esta instalado correctamente. Esto eventualmente será hecho automaticamente por el script update_wormbase.pl, pero es mejor hacerlo manualmente la primera vez para asegurar de que AceDB funciona correctamente.

Esto llevará un tiempo, pero es mejor descargar la distribución C. elegans actual desde:
ftp://ftp.sanger.ac.uk/pub/wormbase/current_release

Descargue todos los archivos dentro de un directorio temp adecuado, como /usr/tmp. Tome todos los archivos llamados database.*.tar.gz, donde * contiene la version de datos actual y el numero de la version del software.

```
% ftp -i ftp.sanger.ac.uk
ftp> type in "anonymous" as username
ftp> ce /pub/wormbase/current_release
ftp> mget database.*.gz
```

Necesitará extraer la base de datos dentro de un subdirectorío de /usr/local/acedb. Eventualmente habrán multiples versiones Acedb aquí con el enlace simbolico apuntando a la version mas reciente. Por convención, el nombre del directorio para arrancar es "elegans_WSXX", donde XX es el numero de version, y el enlace simbolico "elegans" apunta al más reciente:

```
lrwxrwxrwx 1 lstein acedb 29 Jul 23 12:06 elegans ->elegans_WS46/
drwxrwsr-x 8 lstein acedb 4096 May 20 20:42 elegans_WS41/
drwxrwsr-x 8 lstein acedb 4096 May 26 01:31 elegans_WS42/
drwxrwsr-x 8 lstein acedb 4096 Jun 14 14:37 elegans_WS43/
drwxrwsr-x 8 lstein acedb 4096 Jun 22 10:55 elegans_WS44/
drwxrwsr-x 8 lstein acedb 4096 Jul 13 17:55 elegans_WS45/
drwxrwsr-x 8 lstein acedb 4096 Jul 20 01:34 elegans_WS46/
```

Cree el directorio para arrancar correcto y extraiga los archivos tar de la base de datos:

```
% cd ~acedb
% mkdir elegans_WSXX -- reemplaze "XX" con el numero de version
% ln -s elegans_WSXX elegans
```

Nota: Estos comandos estan corriendo bajo los privilegios de usuario normal. Esto funcionará si usted se ha agregado al grupo Acedb y configurado los permisos de directorio como esta descrito arriba.

Ahora extraiga los archivos tar. Asumiendo que los descargó en /usr/tmp, lo siguiente hará el resto:

Sintaxis Bash:

```
cd ~acedb/elegans
for i in /usr/tmp/database*.gz; do gunzip -c $i | tar xvf -;
```

Sintaxis C-shell:

```
cd ~acedb/elegans
foreach i (/usr/tmp/database*.gz)
    gunzip -c $i | tar xvf -
end
```

Esto extraerá los archivos de base de datos dentro de ~acedb/elegans.

Necesitará agregar cuatro archivos de configuracion en ~acedb/elegans/wspec. Ellos son:

| | |
|------------------|---|
| passwd.wrm | Controla el acceso local a los archivos de datos acedb |
| server.wrm | Legaliza el archivo de configuracion para el servidor RPC |
| serverconfig.wrm | Informacion de configuracion para el servidor socket |
| serverpasswd.wrm | Controla el acceso remoto a los archivos de datos acedb |

Encontrará los esqueletos de estos archivos en /usr/local/wormbase/wspec, pero ellos necesitarán ser actualizados con la información de su cuenta local. Realice los siguientes cambios en los archivos originales de /usr/local/wormbase/wspec, y entonces copielos en ~acedb/elegans/wspec. Es importante realizar los cambios a los originales en /usr/local/wormbase/wspec, porque estos archivos son usados por el script de actualización de WormBase para autogenerar nuevas versiones Acedb.

passwd.wrm

Este archivo contiene los nombres de cuenta de los usuarios locales quienes tienen acceso a escritura de la base de datos. Borre lo que este allí (usuario "lstein") y reemplazelo con el nombre de cuenta del administrador (usted). Si quiere ser capaz de actualizar la base de datos a través del servidor socket, agregue al usuario "acedb" a la lista:

```
// passwd.wrm
su_nombre
acedb
```

serverpasswd.wrm

Este archivo contiene los nombres de usuario y contraseñas para todos los que tengan permiso de escritura a la base de datos. Borre estas líneas:

```
admin: admin lstein
write: lstein nchen
```

Reemplazelas por estas líneas:

```
admin: admin
write: su_nombre1 su_nombre2
```

Esto significa que alguien que se conecta con el nombre "admin" y con una contraseña válida tendrá acceso administrativo a la base de datos (habilidad para cambiar contraseñas y apagar el servidor). Alguien que se conecte con el nombre "su_nombre1" o "su_nombre2" tendrá permiso de escritura a la base de datos.

Usted ahora usará el programa makeUserPasswd para crear algunas contraseñas. Cada vez que corra este programa, este imprimirá una contraseña, el cual debería ser manualmente copiado y pegado al pie de serverpasswd.wrm:

```
% ~acedb/bin/makeUserPasswd admin
// Please enter passwd: *****
// Please re-enter passwd: *****
// La siguiente línea es una entrada válida para wspec/serverpasswd.wrm
admin 5b11966a419e057ef0b7b917746e934c
```

Debería hacer esto una vez para el administrador, y una por cada uno de los usuarios que tengan permiso de escritura. Cuando lo haya hecho, serverpasswd.wrm se verá así:

```
// serverpasswd.wrm
admin: admin
write: su_nombre1 su_nombre2
admin 5b11966a419e057ef0b7b917746e934c
su_nombre1 2640075535f3fe296b6797d77bd6a714
su_nombre2 05db4280d9f3b1c1aa6e10479aef4243
```

server.wrm

No necesita configuración extra. Solo copielo en ~acedb/elegans/wspec/

serverconfig.wrm

No necesita configuración extra. Solo copielo en ~acedb/elegans/wspec/

Be sure to copy these changes from the templates in /usr/local/wormbase/wspec to the live database in ~acedb/elegans/wspec!

Llegado a este punto, puede testear si el servidor socket funciona correctamente. Asumiendo que se ha agregado al grupo AceDB, puede correr el siguiente comando:


```
% ~acedb/bin/sgifaceserver ~acedb/elegans
// Database directory: /usr/local/acedb/elegans
// Shared files: /usr/local/acedb
// ##### Server started at 2001-07-23_16:42:31
// ##### host=mondseer.cshl.org listening port=23100
// ##### Database dir=/usr/local/acedb/elegans
// ##### Working dir=/usr/local/acedb/elegans
// ##### clientTimeout=600 serverTimeout=600 maxKbytes=0 autoSaveInterval=600
```

```
// Server listening socket 28 created
```

La línea "listening port=23100" indica que el servidor está escuchando al puerto 23100. Abra una nueva terminal y use saceclient para confirmar que puede comunicarse con el servidor:

```
% ~acedb/bin/saceclient localhost -port 23100
Please enter userid: anonymous
Please enter passwd:
acedb@localhost> find Sequence
// Response: 65 bytes.
```

```
// Found 236493 objects in this class
// 236493 Active Objects
acedb@localhost> quit
// Closing connection to server.
// Client sent termination signal by server.
// Response: 13 bytes.
// A bientot
// Please report problems to acedb@sanger.ac.uk
// Bye
```

La sintaxis de la línea de comandos para saceclient es "saceclient <host> -port <port>". Cuando pida el id de usuario, escriba "anonymous" y simplemente pulse Enter cuando le pida una contraseña. Así entonces emitimos un comando "find Sequence" para contar el número de secuencias en la base de datos (muchas), y "quit" para terminar la conexión.

Ahora testee que la contraseña de admin funcione:

```
~acedb/bin/saceclient localhost -port 23100
Please enter userid: admin
Please enter passwd: *****
acedb@localhost> shutdown now
// Client sending shutdown to server
// Client sent termination signal by server.
// Response: 87 bytes.
// 0 Active Objects
// Sorry, emergency shutdown of server now executing
// A bientot
// Please report problems to acedb@sanger.ac.uk
// Bye
```

Cuando pida el id de usuario, escribimos "admin" y damos la contraseña correcta. El comando "shutdown now" provoca que el servidor cierre. Si nosotros no tenemos privilegios administrativos, deberíamos recibir un error "unknown command" en esta etapa.

4.4) Instalando AceDB para empezar automáticamente

El paso final es configurar el servidor socket Acedb para que empiece automáticamente cuando sea necesario. La forma más típica de hacer esto es usar inetd para arrancar el servidor.

Localice el archivo /etc/inetd.conf, y agregue la siguiente línea al final:

```
2005 stream tcp wait acedb /usr/local/acedb/bin/sgifaceserver \
```

```
sock.acedb /usr/local/acedb/elegans 1200:1200:0
```

Nota: Esta línea fue eliminada al final (con una barra invertida), pero en el archivo de configuración real ni el salto de línea ni la barra invertida deberían aparecer. La primera columna indica a qué número de puerto se escucha. 2005 es el usado por defecto por los archivos de configuración WormBase.

Indíquelo al inetd que recargue su archivo de configuración a través de una señal HUP.

```
# ps -elf | grep inetd
140 S root    500    1 0 60  0  - 329 do_sel Jul17 ? inetd
# killall -HUP 140
```

Usted ahora debería ser capaz de hablar con la base de datos usando saceclient (como un usuario anónimo):

```
% ~acedb/bin/saceclient localhost -port 2005
```

4.5) Instalando Acedb bajo xinetd

¿Qué? ¿No encuentra /etc/inetd.conf? Probablemente está usando un sistema RedHat actualizado que ha reemplazado el probado y funcionando daemon inetd con el (supuestamente más seguro, pero probablemente bugado) daemon xinetd.

Primero, asegúrese de que xinetd aún esté instalado (chequee que se encuentre /usr/sbin/xinetd). Si no, use el administrador RPM (gnorpm o equivalente) para instalar el paquete xinetd (O mejor aún, instale el tradicional inetd). Después de instalar xinetd, asegúrese de que sea el que inicie en el nivel de arranque por defecto del sistema. Use el panel de control de RedHat para esto.

La versión de xinetd que está instalada en RedHat 7.1 no funcionará. Vaya a la sitio de actualizaciones RPM de RedHat e instale xinetd-2.3.7-4.7x. Una vez que xinetd esté instalado, usted ahora necesitará crear un archivo de configuración del xinetd para Acedb. Cree un nuevo archivo llamado /etc/xinetd.d/acedb con el siguiente contenido:

```
# file: /etc/xinetd.d/acedb
# default: on
# description: wormbase acedb database
service acedb
{
    protocol          = tcp
    socket_type       = stream
    port              = 2005
    flags             = REUSE
    wait             = yes
    user              = acedb
    group            = acedb
    log_on_success    += USERID DURATION
    log_on_failure    += USERID HOST
    server            = /usr/local/acedb/bin/sgifaceserver
    server_args       = /usr/local/acedb/elegans 1200:1200:0
}
```

Edite /etc/services. Aunque se supone que xinetd no usa /etc/services, la siguiente línea debe ser agregada:

```
acedb      2005/tcp
```

Reinicie xinetd con el siguiente comando:

```
# /etc/rc.d/init.d/xinetd reload (o restart)
```

Para cerrar xinetd, primero encuentre el id del proceso y entonces:

```
# kill -SIGUSR2 process#
```

Ahora debería ser capaz de hablar con la base de datos usando el saceclient:

```
% ~acedb/bin/saceclient localhost -port 2005
```

Nota: Para saber si el servidor esta escuchando al puerto 2005, corra el siguiente comando:

```
# netstat -ant | grep LISTEN
```

Si salta un error, chequee /var/log/messages, y los archivos serverlog.worm y log.wrm en el directorio actual de la base de datos. Errores comunes incluyen espacio en disco insuficiente y permisos inadecuados para estos dos archivos de registro. Recuerde, el servidor acedb debe ser capaz de escribir estos archivos.

5) INSTALANDO MYSQL

MySQL esta extremadamente bien documentado. Solo siga las instrucciones de instalación y configurelo para iniciar automaticamente cuando el servidor este encendido.

Ejecute el servidor mysql asi:

```
# /etc/rc.d/init.d/mysqld start
```

Primero, configure una contraseña para root asi:

```
# mysqladmin -uroot password PASSWORD
```

WormBase requiere tres conjuntos de base de datos mysql. En el primer conjunto de bases de datos, uno se llama "elegans" y es una base de datos activa. El otro se llama "elegans_load", y es una base de datos temporal usada mientras se cargan nuevas versiones. Esta convención es seguida por las bases de datos llamadas "briggsae/briggsae_load" y "elegans/elegans_load".

En la siguiente guía, el nombre de administrador de mysql es "root" y la contraseña es "PASSWORD". El nombre de usuario actual se asume que es "me". Sustituya estos valores con los adecuados.

Paso 1. Crear la base de datos elegans
mysqladmin -uroot -pPASSWORD create elegans

Paso 2. Crear la base de datos elegans_load
mysqladmin -uroot -pPASSWORD create elegans_load

Paso 3. Darse a si mismo permisos a las bases de datos
mysql -uroot -pPASSWORD elegans
mysql> grant all privileges on elegans.* to me@localhost;
mysql> grant all privileges on elegans_load.* to me@localhost;
mysql> grant file on *.* to me@localhost;

Nota: Esto es una configuración por lo que no tiene que escribir una contraseña para cargar la informacion dentro de estas base de datos siempre que usted este conectado a la maquina de la base de datos. Si quiere una contraseña, necesitará hacer cambios al archivo /usr/local/wormbase/update_scripts/update_wormbase.pl (encuentre las constantes MYSQL_USER y MYSQL_PASS).

Paso 4. Darle al usuario "nobody" permisos de lectura para la base de datos elegans
mysql> grant select on elegans.* to nobody@localhost;

Repita los pasos 1-4 para establecer las bases de datos MySQL "briggsae" y "briggsae_load", y entonces una vez más para "elegans_pmap" y "elegans_pmap_load".

Todas estas tres bases de datos primarias serán pobladas la primera vez que arranque el script update_wormbase.pl. Sobre las actualizaciones subsecuentes, el *_load se volverá temporalmente poblado.

También preste atención a que despues de configurar estas bases de datos, deben seguirse algunos pasos para hacerlos funcionar para Wormbase. Por ejemplo:

Nota: El directorio por defecto para las bases de datos MySQL en RedHat Linux 7.3 es /var/lib/mysql. Asegurese que hay suficiente espacio en /var drive. De otro modo, tiene dos opciones:

1. Ubique las bases de datos en una ruta diferente usando los enlaces simbolicos a /var/lib/mysql.
2. Cambie el directorio por defecto a una ruta diferente en el archivo my.cnf.

6) INSTALANDO LOS MODULOS PERL

La manera más facil de instalar los modulos Perl requeridos es con el shell CPAN en tu directorio home:

```
# perl -MCPAN -e shell
```

La primera vez que lo arranque, pasará por algunos pasos de configuración. Despues de eso, usted estará representado con el "cpan>". Escriba "?" para acceder a la ayuda. Para instalar modulos, escriba "install <module_name>".

Por ejemplo, asi es como se instala el modulo "Bundle::CPAN", el cual esta entre medio de un gran numero de modulos recomendados por CPAN:

```
cpan> install Bundle::CPAN
```

Tendrá que correr los siguientes comandos:

```
cpan> install LWP
cpan> install Net::FTP
cpan> install Digest::MD5
cpan> install Ace
cpan> install XML::Parser
```

El modulo Ace es la version más reciente de AcePerl. Cuando lo instale, le preguntará si construir la version Perl pura, una versión optimizada solo para sockets, o una version optimizada que funciona con sockets y los servidores basados en RPC más viejos. Elija la opcion (2) o la (3).

Cuando instale Ace por primera vez, este también le preguntará si usted quiere instalar AceBrowser. Responda "yes" la primera vez que lo instale (no necesita responder afirmativamente en las subsecuentes actualizaciones). Entonces este le pedirá que elija las rutas para sus archivos de configuración. Para instalaciones WormBase, estos son los valores correctos a elegir:

```
Archivos de configuracion especificas del sitio: /usr/local/wormbase/conf
Ruta CGI: /usr/local/wormbase/cgi-bin
Ruta HTML: /usr/local/wormbase/html
```

El modulo XML::Parser requiere que descargue e instale las expatriadas librerias XML en analisis primero. Esto esta bien explicado en la documentacion que acompaña a la librería expatriada.

El modulo GD actual es un desafío para instalar a causa de sus requerimientos sobre la librería externa libgd. Sin embargo, a causa de las malas versiones, hay demasiadas versiones diferentes de libgd dando vueltas, y algunas no funcionan correctamente con GD. Se sugiere que instale una version mas vieja del modulo GD que viene con su propia librería interna estable. Para instalar la version mas vieja, use este comando:

```
cpan> install LDS/GD-1.19.tar.gz
```

Instale los otros modulos Perl listados antes.

7) INSTALANDO BIOPERL

Puede instalar BioPerl usando CVS anonimo o bien descargando e instalando el nucleo estable más reciente.

7.1) Instalar BioPerl desde la version actual mas estable (recomendado)

```
% wget http://bioperl.org/DIST/current_core_stable.tar.gz
```

```
% gunzip -c cur* | tar xvf -
% cd bioperl-1.4
% perl Makefile.PL
% make
% make test
% sudo make install
```

7.2) Instalando BioPerl desde CVS

Instalandolo de esta manera obtendrá la última versión del BioPerl, pero también podría incluir bugs sin resolver y código experimental.

```
% cvs -d :pserver:cvs@cvs.open-bio.org:/home/repository/bioperl login
    cuando pida la contraseña, escriba 'cvs'
% cvs -d:pserver:cvs:cvs@cvs.open-bio.org:/home/repository/bioperl co bioperl-live
% cd bioperl-live
% perl Makefile.PL
% make
% make test
% sudo make install
```

Esto creará un directorio con el nombre bioperl-live. En el futuro, cuando desee actualizar a la versión más reciente, simplemente escriba "cvs update" en el directorio bioperl-live.

7.3) Instalando BioPerl de la forma usual

Ejecute "perl Makefile.PL", "make", "make test" y "make install".

8) INSTALANDO GENERIC GENOME BROWSER

Este es un script CGI que contiene algunos módulos Perl que usan Bio::DB::GFF y Bio::Graphics para crear el proyector principal de genomas de WormBase. Se encuentra en www.gmod.org. Como con BioPerl, GBrowse puede ser instalado por CVS anónimo o desde la última versión más estable.

Por CVS:

```
% cvs -d:pserver:anonymous@cvs.gmod.sourceforge.net:/cvsroot/gmod login
    Cuando pida una contraseña para anonymous, simplemente presione Enter.
% cvs -d:pserver:anonymous@cvs.gmod.sourceforge.net:/cvsroot/gmod \
    co Generic-Genome-Browser
```

A través de la última versión estable:

```
% wget http://umh.dl.sourceforge.net/sourceforge/gmod/Generic-Genome-Browser-X.XX.tar.gz
    Donde X.XX es la versión más estable.
% gunzip -c Gene* | tar xvf -
```

Escriba el directorio de extracción o el indicado por CVS y ejecute los siguientes comandos para instalarlo en el lugar apropiado para WormBase:

```
perl Makefile.PL HTDOCS=/usr/local/wormbase/html \
    CGIBIN=/usr/local/wormbase/cgi-perl/seq \
    CONF=/usr/local/wormbase/conf \
make
make install
```

9) INSTALANDO APACHE Y MOD_PERL

Instalar Apache/mod_perl es exactamente igual a como se describe en la documentación que acompaña a estos paquetes. Sin embargo, debe ser cuidadoso al usar el Makefile.PL del mod_perl para configurar y construir Apache, cuando esto desactiva la librería expatriada interna que viene con Apache. De otro modo, será incapaz de arrancar las páginas de WormBase que se basan en el análisis XML.

Extraiga Apache y mod_perl dentro de dos directorios de lado a lado:

```
%ls
drwxr-xr-x  8 lstein lstein  4096 Jul 16 15:42 apache_1.3.17/
drwxr-xr-x 24 lstein lstein  4096 Jul 16 14:45 mod_perl-1.25/
```

Escriba el directorio mod_perl, y ejecute este comando

```
% perl Makefile.PL DO_HTTPD=1 USE_APACI=1 EVERYTHING=1 \
    APACHE_PREFIX=/usr/local/apache \
    APACI_ARGS='--enable-shared=info --enable-shared=status'
```

La opción APACI_ARGS en este comando prende dos modulos Apache que brindan informacion del estado. Ellos no son estrictamente necesarios para WormBase.

Usted tendrá muchisima informacion de diagnostico. Ahora ejecute los siguientes dos comandos:

```
% make
% make test
```

La librería LWP debería estar instalada antes del "make test". Si el test es satisfactorio, pase a root y ejecute:

```
# make install
```

Esto instalará Apache dentro del directorio /usr/local/apache.

Nota: si usted tiene problemas instalando Apache/mod_perl, podria probar instalando versiones más viejas de ellos. Apache_1.3.26 y mod_perl-1.27 funcionan bien con Red Hat 7.3.

10) CONFIGURANDO WORMBASE

10.1) Configurando httpd.conf

En /usr/local/wormbase/conf/httpd.conf, encontrará un archivo de configuracion Apache conteniendo definiciones especificas de WormBase. Usted puede copiar y pegar este archivo dentro del archivo de configuracion principal (/usr/local/apache/conf/httpd.conf), reemplazando las directivas ya escritas allí, o, mejor, use una directiva Include para traer a estas directivas dentro.

Si WormBase va a ser el único sitio web hospedado por este servidor, entonces elimine todas las secciones DocumentRoot y <Directory> desde el archivo de configuración principal. Cambie la directiva de Port a "Port 80", y escriba esto al final del archivo:

```
Include /usr/local/wormbase/conf/httpd.conf
```

Si WormBase esta por ser un host virtual (uno de los muchos sitios web hospedados por el servidor), entonces debe crear una seccion <VirtualHost> apropiada. Aquí hay un template de ejemplo:

```
<VirtualHost 143.48.220.84:80>
ServerName www.wormbase.org
UseCanonicalName on
Include /usr/local/wormbase/conf/httpd.conf
</VirtualHost>
```

La direccion IP en la etiqueta <VirtualHost> debe ser reemplazada por la dirección IP correcta para el servidor. Igualmente, el ServerName debe ser reemplazado por un nombre DNS que resolverá correctamente la dirección IP. ¡No use "www.wormbase.org"! Este nombre ya esta tomado.

Las directivas en /usr/local/wormbase/conf/httpd.conf harán lo siguiente:

1. Establece /usr/local/wormbase/html como el documento raiz para los archivos HTML estaticos.
2. Establece /usr/local/wormbase/db como un directorio script bajo el control de Apache::Registry del mod_perl.

3. Crea logs de errores y transferencia en `/usr/local/wormbase/logs`.
4. Crea un directorio `cgi-bin` común en `/usr/local/wormbase/cgi-bin`.
5. Ponga todos los archivos estaticos `.html` bajo el control de `Apache::AddWormbaseBanner`, un módulo que añade el encabezado y pie de página estandar de WormBase a todos los archivos HTML.

`/usr/local/wormbase/conf/httpd.conf` no debería necesitar ningun ajuste, excepto uno: la localización del directorio para puesta en escena para imagenes generadas dinamicamente. Este incluye las siguientes directivas:

```
Alias /ace_images /var/tmp/ace_images
```

El directorio `ace_images` será creado automaticamente la primera vez que WormBase lo necesite, pero el directorio que contiene, en este caso `/var/tmp`, debe poder ser escrito por el usuario Apache (usualmente "nobody"). Las imagenes eventualmente ocuparan aproximadamente 10 MB. Si `/var/tmp` no es apropiado para su sistema, cambie el segundo argumento hacia alguna localizacion que sea mas adecuada.

10.2) Configurando `elegans.pm` y `localdefs.pm`

WormBase usa dos archivos principales de configuracion, `elegans.pm` y `localdefs.pm`, localizados en `/usr/local/wormbase/conf`.

El primero, `elegans.pm`, contiene una variedad de definiciones Perl que son usadas por los muchos scripts WormBase `mod_perl`. Analice estos archivos, pero probablemente no necesitará realizar ningun cambio. El único objeto que podría querer cambiar es el que controla la localización de los archivos temporales:

@PICTURES

Esta es la localización de un directorio temporal de puesta en escena para imagenes generadas dinamicamente como se indica en `conf/httpd.conf`. Su valor es una lista en la cual el primer objeto es donde las imagenes aparecerán en el servidor Web (en espacio URL) y el segundo objeto es donde aparecerán en el sistema de archivos:

```
@PICTURES = ('/ace_images' => '/var/tmp/ace_images');
```

Si usted cambio la localización del directorio de puesta en escena en `httpd.conf`, debe realizar los cambios pertinentes aquí.

El segundo archivo, `localdefs.pm`, contiene hostnames especificos del sitio, puertos, y contraseñas. Encontrará un template para este archivo en `/usr/local/wormbase/conf/localdefs.pm.template`. Renombre este archivo `localdefs.pm` y edite las siguientes opciones por las adecuadas para su sitio.

\$HOST

Este es el nombre del host donde el servidor socket arranca. Establecido como "localhost" por defecto.

\$PORT

Este es el puerto sobre el cual el servidor socket arranca, 2005 por defecto.

\$ACEPASS, \$USERNAME, \$PASSWORD

Estos tres definen el nombre de usuario y la contraseña de `acedb`.

\$MYSQL_HOST, \$MYSQL_USER, \$MYSQL_PASS

Estos tres definen el host, nombre de usuario y contraseña de `mysql`.

\$MASTER

Esto es usado solo para el sitio maestro de WormBase. Debería ser 0.

\$MIRROR

Si el sitio es o no es un mirror. Se debería establecer el nombre del mirror.

\$DEVELOPMENT

Si el sitio es uno es un sitio en desarrollo. Internamente, esto controla la naturaleza de la memoria caché en el sitio. Debería ser 0.

\$BLAST2WORMBASE, \$WORMBASE2BLAST

Estas dos opciones controlan donde el script BLAST direcciona las consultas, y donde devuelven los resultados. Esto ocurre en el evento en que un segundo servidor BLAST independiente es previsto. Si no, estas dos opciones deberían apuntar a:

```
$WORMBASE2BLAST=http://yoursite.tv
```

10.3) Reiniciando WormBase

Cuando los archivos de configuración han sido chequeados y ajustados, reinicie Apache con el siguiente comando:

```
# /usr/local/apache/bin/apachectl restart
```

Busque en `/usr/local/wormbase/logs/error_log` (errores específicos de WormBase) y `/usr/local/apache/logs/error_log` (errores generales) cualquier mensaje de error. Si no hay ninguno, trate de abrir la página principal. Usted debería ver un banner y un pie de página de WormBase. Las distintas búsquedas en las bases de datos deberían funcionar también. Sin embargo, las páginas precomputadas "genome dump" no funcionarán aun porque ellas no han sido generadas.

10.3.1) Si no funciona

Hay unos cuantos problemas comunes que chequear:

¿El servidor socket acedb esta arrancando?

Ejecute "ps" para determinar si el servidor esta sin dudas arrancando. Si no lo esta, regrese a la sección de configuración de AceDB y confirme que todo esta donde debería estar. Asegurese de que sea posible escribir el directorio `/usr/local/acedb/elegans/database` por los usuarios AceDB.

Analice los dos logs acedb para buscar mensajes de error, ambos estan en `/usr/local/acedb/elegans/database`. Examine `log.wrm` y `serverlog.wrm`.

¿El servidor acedb esta crasheandose?

Es posible que el servidor se crashee pronto despues de iniciarse. El por que de esto se debe a que el sistema se pone muy ocupado por un momento, y "top" o "ps" muestran el servidor reiniciandose repetidamente. Eventualmente, inetd (o xinetd) inhabilitará al servidor y emitirá un mensaje syslog por el hecho de que esta inhabilitando un servicio "en bucle".

De nuevo, chequee que el acedb este instalado correctamente y que el directorio de la base de datos pueda ser escrito. Chequee `log.wrm` y `serverlog.wrm`.

"Internal Server Error"

Esto es típicamente un sintoma de que el `mod_perl` no esta instalado correctamente, una librería Perl esta faltando, o algo esta mal con la configuración. Analice los dos archivos de `error_log` (en `/usr/local/apache/log` y `/usr/local/wormbase/log`) por pistas.

El banner se muestra pero las pequeñas imagenes decorativas estan rotas

En algunas versiones de Linux corriendo la librería `libc 2.2` existe un bug en `readdir()`, que es la función llamada para leer los contenidos del directorio. Usted puede chequear que versión de `glibc` tiene buscando en los contenidos de `/lib`:

```
% ls -l /libc-*  
-rwxr-xr-x 1 root root 4101324 Feb 29 2000 /lib/libc-2.1.3.so*
```

Las versiones que esten en situacion de riesgo mostrarán `libc-2.2.so` instalado. La solución es actualizarse a una versión más reciente de `libc`, `libc 2.2.3` funciona correctamente.