Free-Vote: Manual de Instalación

Juan Antonio Martínez Castaño *jonsito@teleline.es* v1.1, Enero 2001

Este documento incluye instrucciones para compilar e instalar el sistema de voto electrónico **Free-Vote**.

Índice General

1 Copyright

Este programa, su código y documentación, son Copyright © 2000 de Juan Antonio Martínez Castaño

Free-Vote es distribuído bajo los términos y condiciones de la Licencia Pública General de GNU *(GPL)*

2 Introducción

Free-Vote ha sido diseñado para servir y dar soporte a sistemas de votación electrónica con un nivel razonable de seguridad y fiabilidad

Las características principales de ***Free-Vote*** son:

Independiente del navegador

Diseñado completamente en HTML-3.0, se ha omitido expresamente el uso de javascript, applets, plugins, etc en aras de una mayor simplicidad y portabilidad

Multiconsulta

Se pueden realizar y monitorizar simultáneamente varias consultas

Configurable

Cada consulta tiene diversos parámetros, definibles por el organizador de la consulta:

- Consulta pública o restringida
- Contenido del voto público o secreto
- Cada consulta lleva parejo un foro de debates, en el que los usuarios pueden enviar comentarios y sugerencias
- Posibilidad de definir los periodos de notificación, registro, y votación
- Control de información disponible durante la consulta:
  - Saber si un votante ha votado o no
  - Datos sobre porcentajes de participacion
  - Datos sobre resultados parciales de la consulta
- Selección y definición de las opciones de voto

Autentificación de votantes

Cada votante recibe al realizar la acreditación una *tarjeta* de voto, válida una única vez

Garantía de voto único y secreto

El sistema sólo registra si el usuario ha votado o no, nunca el valor de su voto

Control de acceso

En consultas privadas sólo tienen derecho a voto aquellos votantes definidos por el organizador.

Posibilidad de supervisión

Las consultas pueden llevar asociados uno o varios supervisores, que reciben vía correo electrónico los eventos asociados a la votación requerida

Uso de SSL y Certificados Digitales

Existe soporte para conexiones seguras, así como la autentificación mediante la presentación de certificados digitales desde el navegador

Realimentación mediante correo electrónico

El usuario recibe respuesta a sus operaciones a través del correo electrónico. En función de la configuración del sistema, éste puede utilizar encriptación PGP para enviar el correo

Seguimiento y registro de eventos

Free-Vote utiliza *syslog(2)* para el registro de eventos. A su vez, es posible especificar nivel de registro en función del evento generado

Puesto que el votante no tiene garantía de que realmente este sistema haga lo que se afirma, existe en todo momento un grupo de usuarios ajeno a este web, que supervisa los contenidos y funcionamiento, dando garantía de "buena fe". Se está considerando la posibilidad de elaborar un sistema de signado electrónico para control de integridad y autenticidad del software

Free-Vote Está basado en *PHP-3.0* y *PostgreSQL-7.0.* Una copia de la última versión del código fuente está disponible vía web en *http://drake.dit.upm.es/~jantonio/e-vote/evote.tgz*

De conformidad con el Real Decreto 994/1999 de desarrollo del Reglamento de Seguridad de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos (LORTAD), este fichero puede ser considerado el Documento de Seguridad exigido por dicho reglamento. Debido a la naturaleza meramente identificativa de los datos contenidos en la base de datos solamente son requeridas las medidas asociadas al nivel de seguridad básico, y que son descritas y desarrolladas en el manual de usuario

Free-Vote Se distribuye bajo *Licencia GPL.*

3 Antes de empezar

Antes de empezar es preciso comprobar que se dispone en el sistema de los siquientes paquetes instalados y configurados

1. Servidor Web Apache versión 1.3.9 o superior.
2. PHP 3.0.12 o superior. FreeVote no está probado con las versiones 4.X de PHP, por lo que no se garantiza su funcionamiento (feedback agreeded :)
3. PostGreSQL 7.0.0 o superior. Está previsto en un futuro el soporte de otros sistemas de RDBMS
4. Si se van a utilizar conexiones seguras, necesitaremos Apache-SSL, con los módulos mod_ssl y el paquete OpenSSL versión 0.9.5a o superior. En la dirección *http://www.modssl.org* encontraremos toda la documentación necesaria, así como los paquetes de software requeridos
5. Si se van a usar certificaciones digitales, puede ser necesario el considerar la configuración de un servidor de certificaciones (CA o certification authority). los paquetes OpenCA o PyCA cumplen perfectamente este cometido
6. Servidor de correo. En principio cualquier MTA servirá para nuestros propósitos
7. Si vamos a utilizar PGP para firmar y encriptar los mensajes salientes deberemos instalar dicho soporte. PGP o GnuPG son ambas opciones válidas y soportadas por el sistema

Si no sólo queremos instalar el paquete, sino compilarlo, necesitaremos además las siguientes herramientas:

1. LinuxDoc-SGML para compilar y generar la documentación
2. Gif-Tools para procesar los diversos gráficos de la documentación
3. Compilador de C gcc o egcs correctamente instalado

El paquete FreeVote se distribuye tanto en fuentes (.tgz o .src.rpm) como en formato .rpm. La dirección donde obtener el paquete es *http://freevote.sourceforge.net*

Una versión beta, con las últimas modificaciones, puede ser obtenida en *http://drake.dit.upm.es/free-vote*

4 Compilando e instalando Free-Vote

Si partimos del código fuente, la primera operación a realizar es la *compilación*

Para ello, procederemos como sigue:

- Si se parte de el fuente en formato *.tgz* basta con descomprimir el fichero y ejecutar: "make"
- Si se parte del fuente en formato *.src.rpm* lo instalaremos y compilaremos con las rpm-tools, generando el fichero *.i386.rpm* asociado

La instalación es un poco más compleja:

Por defecto, FreeVote instala su árbol de ficheros bajo el directorio */usr*. En el caso de querer mantener este convenio, ejecutaremos: *make install* para el caso del fuente en .tgz, o bien *rpm -v -i freevote-1.1-0.i386.rpm* para el caso del paquete en formato .rpm

Si queremos cambiar el directorio de instalación, deberemos , bien ejecutar *make PREFIX=_nuevo_directorio_ install*, en el caso de partir de un fichero *.tgz* o bien editar el fichero *.spec* y efectuar un *rebuild* en el caso de distribución en formato *.rpm*

Esta instalación deja mucho de ser completa: FreeVote no es sino un conjunto de templates y bibliotecas que interaccionan con diversos servicios del sistema. Es preciso configurar esta interrelación correctamente antes de poder utilizarlo. El proceso se detalla en el siguiente apartado

5 Configuración de Free-Vote

Una vez instalado FreeVote, es preciso proceder a su correcta configuración. Examinaremos paso por paso los apartados respectivos.

5.1 El fichero de configuración

El primer paso consiste en la creación del fichero de configuración. Para ello se debe copiar el fichero */etc/freevote.conf.dist* en el fichero */etc/freevote.conf*, y proceder a la edición de éste.

El fichero de configuración no es sino una secuencia de asignaciones de variables a valores. A continuación se describen éstos y sus significados:

1. Directorios y URLs

TMPDIR
: Directorio donde se almacenan datos y ficheros temporales. Deberá tener permisos de escritura para el usuario bajo el que se ejecute el servidor web (normalmente *nobody* o *www*

FREEVOTE_INST
: Directorio base de la instalación de FreeVote. Normalmente (a menos que se haya cambiado dicho directorio, tal y como se explica en el capítulo anterior) contendrá el valor */usr*

APACHE_CONF
: Directorio donde reside el fichero de configuración del servidor Apache.

INSTALLDIR
: Directorio del sistema de archivos donde se deben instalar las páginas web de FreeVote durante el proceso de personalización

WEBURL

URL desde la que van a ser accedidas las páginas Web de FreeVote. WEBURL debe estar en el fichero de configuración de Apache direccionada a INSTALLDIR (ver apartado sobre configuración del web)

2. Configuración del gestor de informes y backups

SYSLOG

Indica la *facility* a la que se van a asociar los eventos de syslog() generados por FreeVote. Para más detalle consultar la página de manual **syslog(3)**

LOGDIR

Directorio donde se almacenan los ficheros de logging de FreeVote.

BACKUPDIR

Directorio donde se almacenan los backups de FreeVote

Además existen una serie de variables **EVENT_XXXX**, que definen los diversos tipos de eventos que pueden generarse, así como los niveles de verbosidad en la generación de informes sobre dichos eventos. Para más información, cnsultar el apartado correspondiente a la configuración del registro de sucesos

3. Variables de entorno

USE_HTTPS

Indica si se debe utilizar el protocolo HTTPS para el acceso a páginas con información susceptible de ser monitorizada

USE_PGP

Indica si nuestro sistema tiene instalado soporte de encriptación de correo, y si éste es PGP o GnuPG

PGP_PASSWD

Contraseña de desbloqueo para poder firmar digitalmente los mensajes generados (ver sección referida al correo y a la configuración de PGP)

4. Configuración de la base de datos

DBTITLE

Nombre "genérico"que le damos al sistema de voto una vez instalado (eg "Votaciones ACME S.L."

DB_PROGRAM

Nombre del servidor de bases de datos que utilizamos. En el momento actual solo se soporta PostGreSQL

DBNAME

Nombre de la base de datos que contiene la información de FreeVote

DBUSER

usuario propietario de la base de datos . Notesé que se refiere a un usuario PostGreSQL, no necesariamente a un usuario del sistema

DBPASSWD

contraseña de acceso a la DB por parte del usuario anterior

DBHOST y DBPORT

Servidor y puerto de acceso en el que reside la base de datos

5. Datos administrativos. Se incluyen aquí los datos referidos a nombre, apellidos, etc del administrador de la base de datos. FreeVote utiliza estos datos para crear el superusuario del sistema

Como es obvio, dadas las características de los datos contenidos en este fichero, deberá estar instalado en modo de solo lectura para el usuario *root*

5.2 Instalación de las páginas web

Una vez editado el fichero de configuración, el siguiente paso es compilar e instalar los templates de las páginas web extraídas del paquete, así como de generar diversos ficheros auxiliares.

El método mas sencillo es utilizar el programa de instalación previsto a tal ejemplo. Supondremos de ahora en adelante que FreeVote se ha instalado en el directorio /usr. y procederemos a ejecutar:

/usr/bin/freevote_install.sh –install-files

Dicho programa realiza las siguientes tareas:

- Genera la jerarquía de directorios necesaria
- Copia los scripts y programas en su ubicación definitiva
- Personaliza los diversos ficheros que deben interactuar con el resto de los sistemas del servidor (crontab, httpd, syslog, php)
- Crea una copia de seguridad de la instalación y la deposita en **INSTALLDIR**
- Copia los ficheros más relevantes en BACKUPDIR

  En el caso de que el usuario desee realizar estas tareas a mano, se deberá examinar el código fuente del proceso de instalación y proceder según se detalla. No obstante, esta operación no se recomienda, por no ser realmente necesaria

5.3 Configuración del Servidor de Bases de Datos

La configuración del servidor de bases de datos, es sin duda la parte más complicada de la instalación. Por ello, se han previsto una serie de scripts para facilitar la labor. No obstante, y puesto que en ocasiones (por ejemplo en caso de caida del sistema y necesidad de una recuperación manual) será necesario realizar alguna de estas tareas a mano, procedemos a describirlas en detalle.

5.3.1 Creación del usuario operador del sistema FreeVote.

FreeVote accede a la base de datos a través del usuario definido como **DBUSER** y con la contraseña **DBPASSWD** tal y como figuran en el fichero de configuración.

La creación del propietario de la base de datos puede realizarse de dos maneras:

- A través del programa de instalación:

  /usr/bin/freevote_install.sh –create-user

- A mano:
  1. Entrar como usuario postgres
  2. Ejecutar el comando *createuser(1)* y crear un usuario con derecho a crear bases de datos pero no a añadir nuevos usuarios
  3. Ajustar la contraseña con el comando *pg_passwd(1)*

5.3.2 Creacion de la base de datos y sus declaraciones

Al igual que en el apartado anterior podemos realizarlo, bien a mano, bien mediante un script

- A través del programa de instalación:

  /usr/bin/freevote_install.sh –restart-db

- A mano (substituír DBUSER por el usuario creado en el paso anterior):

  1. Entrar como usuario postgres
  2. Crear la base de datos:

     createdb freevote -U DBUSER
  3. Si tenemos la versión 7.0.0 de PostGreSQL, será necesario añadir el soporte de lenguaje PL/PgSQL

     createlang -U postgres -L /usr/lib/pgsql plpgsql freevote
  4. Crear las estructuras de la base de datos:

     psql freevote -U DBUSER -f /usr/lib/freevote/lib/database.sql

5.3.3 Creación del usuario administrador de FreeVote

FreeVote soporta diversas categorías de usuarios. El más destacable es el administrador. Los datos de éste son definidos en el fichero de configuración. Para crear dicho usuario Ejecutaremos el comando:

/usr/bin/freevote_install.sh –register-sysop

El programa toma los datos del fichero de configuración, registra el usuario, y le asigna una contraseña aleatoria, que se guarda en la copia de seguridad del fichero de configuración que se almacena en BACKUPDIR.

No es recomendable el crear este usuario a mano, pues se debe garantizar que tenga userid=1 y groupid=6. En caso necesario, procedase a estudiar el script de instalación para realizar esta tarea

5.4 Sistema de correo

Las operaciones de personalización del correo se reducen a ajustar las opciones referidas al gestor de correo existentes en el fichero */etc/httpd/php3.ini*, y a preparar el soporte de firma y encriptación PGP en caso de que éste se vaya a utilizar.

Es preciso, en el caso de que se desee soporte PGP/GnuPG, que la direccion de correo **ADMIN_EMAIL** tenga generadas y definidas las claves pública y privada en el anillo de claves que utiliza *FreeVote*. En la sección correspondiente a la configuración de PGP/GnuPG se detalla el procedimiento

NOTA:*En el momento actual PGP no está soportado , debiendo utilizar GnuPG si se desea firmado digital de los mensajes*

5.5 Soporte PGP/GnuPG

Free-Vote Incorpora la posibilidad de firmar y encriptar los mensajes generados por el sistema, de manera que se certifique el origen de éstos. Esto es necesario especialmente en las operaciones relacionadas con la intervención de una votación.

*NOTA: En el momento actual, **FreeVote** no soporta PGP, sino sólo GnuPG. Del mismo modo no está habilitada la opción de encriptar los mensajes, funcionando solamente la firma de éstos*

La variable ***USE_PGP*** del fichero de configuración indica el programa a utilizar. Seleccionaremos **"NONE", "PGP",o "GnuPG"**

, según sea nuestro caso

El siguiente paso es crear las estructuras y directorios necesarios para el funcionamiento del soporte PGP desde el servidor Web: Los mensajes generados por ***Free-Vote*** van firmados por el usuario **ADMIN_EMAIL**, por lo que es necesario crear y exportar las claves para dicho usuario

El script de instalación *freevote_install.sh* contiene la opción *–install-pgp* que realiza las opereciones necesarias:

- Crear los directorios adecuados
- Crea los anillos de claves
- Exporta a un servidor de claves la clave pública del usuario **ADMIN_EMAIL**. El administrador deberá proporcionar la dirección de un servidor de claves PGP accesible desde el servidor de voto
- Ajusta los permisos para que el usuario *nobody* pueda acceder a los anillos desde el servidor web

Si bien es posible realizar las operaciones de forma manual, se recomienda utilizar el script proporcionado para ello

BUG: La versión actual de freevote, presupone que los ejecutables de gpg y pgp residen en */usr/bin*. En caso de que esto no sea así será preciso editar el fichero *tools.php3* y corregirlo

5.6 Sistema de eventos y *logging*

El programa de personalización habrá configurado correctamente el fichero */etc/syslog.conf*. Comprobaremos este punto, y en el caso de que todo sea correcto se deberá proceder a relanzar el demonio de syslog

FreeVote define diversos tipos de evento, asociados cada uno a un tipo de operaciones sobre el sistema:

EVENT_AUTH
: Autentificacion de usuarios

EVENT_ADMIN
: Operaciones de administracion

EVENT_ACCESS
: Registro de accesos al web

EVENT_VOTE
: Operaciones de voto y solicitud de clave

EVENT_REGISTRY
: Registro de usuarios, consultas e interventores

EVENT_DEBUG

Operaciones de sistema, trazas, etc

Cada una deberá estar previamente definida en el fichero de configuración con el nivel adecuado, acorde con el comando *syslog(3)*. Para la mayor parte de las instalaciones, la configuración propuesta será la correcta

5.7 SSL y Certificación digital

La variable **USE_HTTPS** del fichero de configuración, indica al sistema si se desea o no el uso de conexiones SSL para poder operar con FreeVote. Un valor de '0' (cero) hará que no se utilicen conexiones seguras en el sistema, activándose si dicha variable tiene el valor '1' (uno)

Si tenemos instalado el soporte para SSL y además el de certificación digital podemos proceder a personalizar la configuración para la aceptación de certificados digitales. Para ello, editamos el fichero */etc/httpd/conf/httpd.conf.freevote*, generado en el proceso de instalación y ajustamos el valor de la variable SSLVerifyClient. Existen las siguientes opciones:

none

No se requiere el uso de certificación digital

optional

Se le pide certificado al cliente, pero se permite continuar la ejecución si no es presentado el certificado

required

Es precisa la presentación de un certificado digital para poder acceder a las páginas

Para poder utilizar certificados digitales, el sistema debe estar correctamente instalado y configurado. Se remite al lector a las páginas del manual sobre mod_ssl y OpenSSL, para la configuración del resto de parámentros del soporte SSL

5.8 Ajuste del *crontab* y gestión de tareas periódicas

Verificar que el programa de instalación ha modificado correctamente el fichero crontab del usuario *root*. En caso necesario, se almacena en BACKUPDIR una copia de las entradas del crontab asociadas a FreeVote

5.9 Pruebas finales

Una vez realizado este proceso, procederemos a relanzar el servidor web y el servidor de bases de datos. Accediendo al navegador a la página principal (definida como WEBURL) , deberemos obtener la página de bienvenida. Comprobaremos, accediendo a los menús de consultas que el acceso vía SSL funciona correctamente, y que el acceso a la base de datos tampoco da problemas.

En caso necesario se proporciona un script de ejemplo */usr/lib/freevote/lib/ejemplo.sql* , con una serie de usuarios y consultas predeterminadas. El operador puede jugar con este script para familiarizarse con el sistema antes de ponerlo en producción

Es muy importante que el operador recuerde que en caso de modificar el fichero de configuración, será preciso reinstalar el sistema, o al menos aquellas partes que se hayan visto afectadas. En concreto el comando

/usr/bin/freevote_install.sh –install-files

será necesario ejecutarlo siempre, pues es preciso reconstruír unos ficheros internos necesarios para el funcionamiento del servidor PHP

6 Programa de instalación

7 Para más información

7.1 Consideraciones de seguridad

7.2 Enlaces y referencias

7.3 Pruebas iniciales. Aplicaciones de ejemplo