FoxPress – Enero 2005

Instalación segura de Firebird en Win 2003 Server

Por Simon Carter

TECT Software Ltd

http://www.tectsoft.net/

Instala Firebird 1.5.x. (para más información sobre si instalar la versión clásica o superserver puedes mirar este link http://ibphoenix.com/main.nfs?a=ibphoenix&l=;PAGES;NAME='ibp_ss_vs_classic').

SYSDBA

Por defecto FB viene con una cuenta llamada SYSDBA. La clave de La clavepor defecto para el usuario SYSDBA es masterkey.

Cambia la clave de SYSDBA a alguna otra cosa más segura. Para cambiar la clave inicia una sesión de DOS, cambia la carpeta a FB_Install y escribe lo siguiente:

```
gsec -user SYSDBA -pa masterkey -modify SYSDBA -pw <new password>
```

Donde <new password> es el password que te gustaría aplicar a la cuenta SYSDBA.

Nota: Sólo son relevantes los primeros 8 dígitos del password, si cuando cambies el tamaño del password el tamño del nuevo password es más grande que 8 dígitos verás el siguiente aviso:

```
Warning - maximum 8 significant bytes of password used
```

Este warning se puede ignorar.

Firewall

Por defecto FB usa el Puerto 3050, si estás usando un firewall entonces necesitarás abrir este puerto para que tus usuarios puedan acceder a sus bases de datos externamente.

Alias's

FB tiene la capacidad de usar Alias, esto te dará más seguridad pues no es necesario que los usuarios sepan el nombre del directorio y su path y de esta forma pueden usar el alias del nombre para conexión.

Los Alias se guardan en 'aliases.conf' que se puede encontrar dentro del path de instalación de FB. Las entradas tienen el siguiente formato:

```
AliasName = drive:\path to database\databasename.fdb
```

Seguridad

Para asegurar Firebird necesitarás primero correr el servicio dentro del contexto del usuario y cambiar los permisos de la carpeta. Esto conlleva crear una cuenta de usuario en Windows y modificar los permisos de una unidad NTFS o de una carpeta.

Seguridad de Usuario

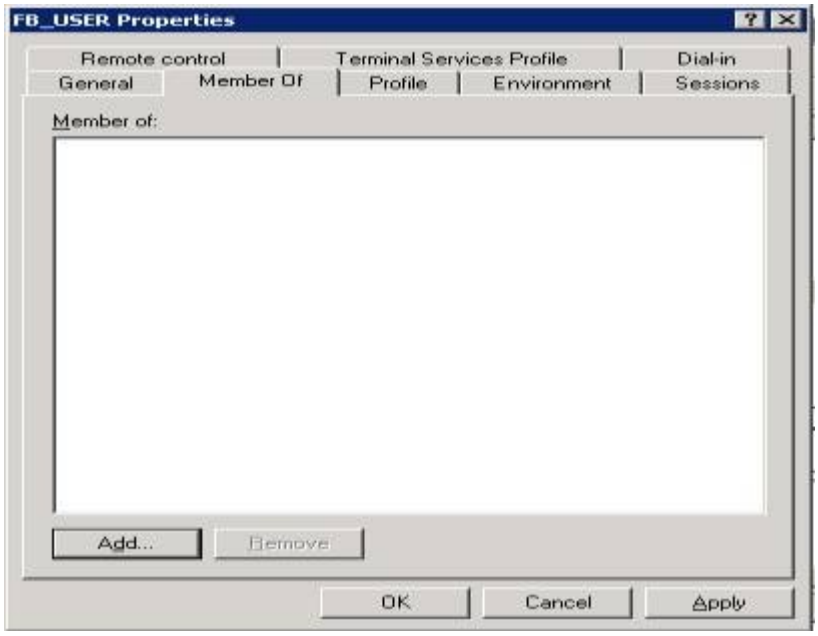
Es important crear un usuario para ejecutar Firebird, esto ter permitirá asegurar al servidor mediante permisos NTFS.

Creación de un usuario

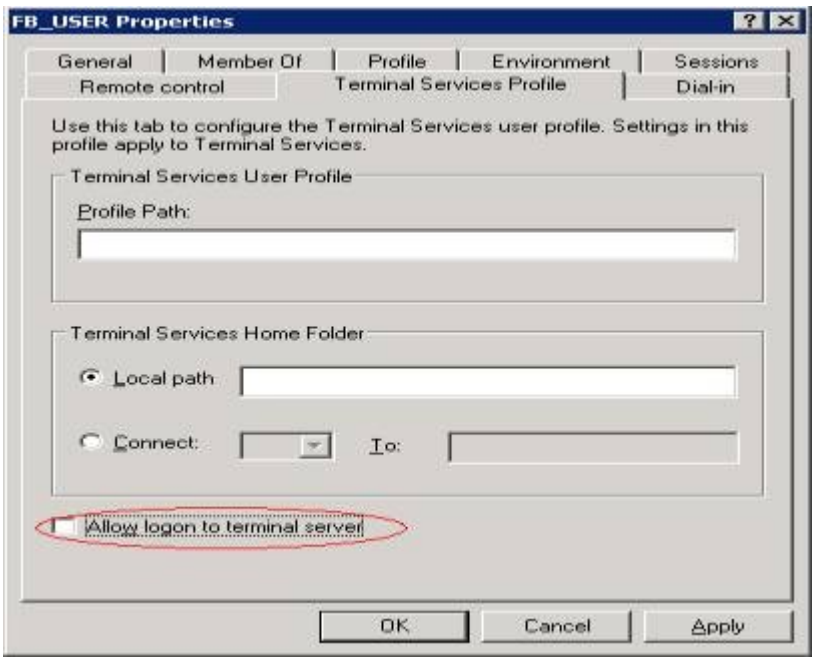
Ve al Panel de Control > Herramientas Administrativas > Computer Management, selecciona 'Usuarios Locales y Grupos', y a continuación selecciona 'Users' desde el arbol de la izquierda dentro de la pantalla de Administración.

Haz clic con el botón derecho del ratón en 'Usuarios' y selecciona 'Nuevo Usuario', se te presentará la siguiente ventana de diálogo. Create un usuario, para este ejemplo crearemos un usuario con el nombre 'FB_USER'. Asignale un password y selecciona el 'Password nunca espira' y pulsar en Crear.

Click Cerrar para cerrar la ventana de nuevo usuario. Dentro de la ventana de Administración de usuarios, haz click en la cuenta recientemente creada de FB_USER, esto te abrirá la ventana de propiedades del usuario. Selecciona la pestaña de 'Member Of' y quita todos los grupos de usuarios.



Ahora selecciona la pestaña de 'Terminal Services Profile'.

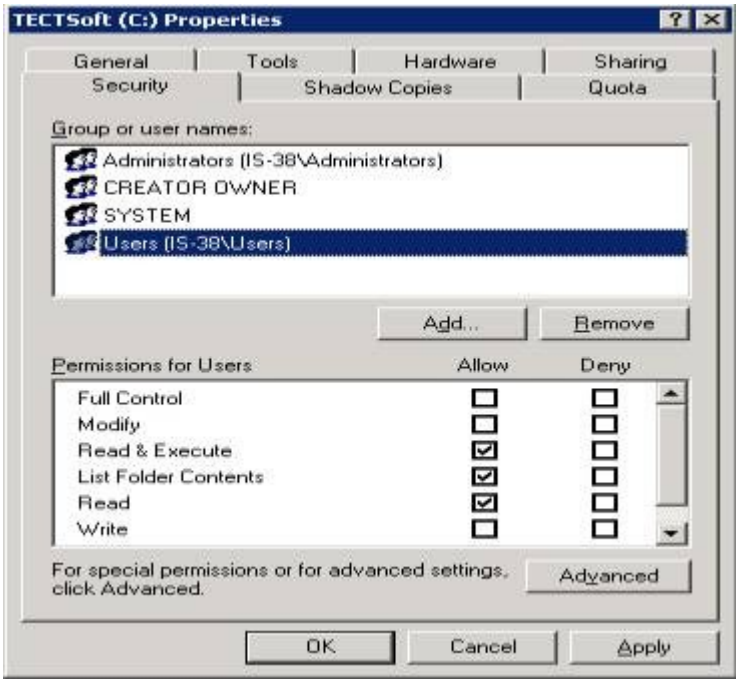


Asegurate de que está desmarcado el check box ‘Allow logon to terminal server’, y haz click en OK.

Seguridad de acceso al disco y a las carpetas

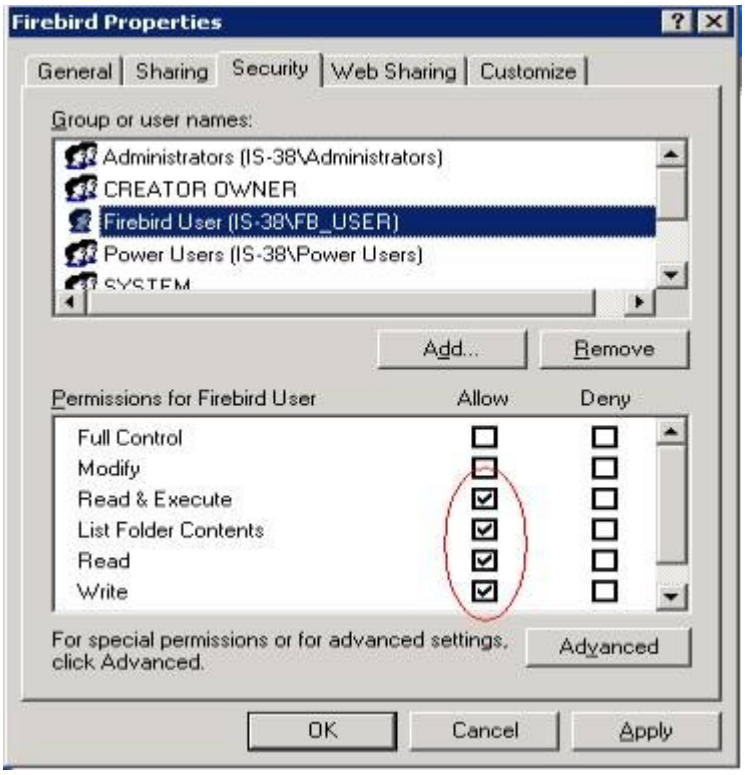
Para evitar que los usuarios puedan crear Bases de Datos en cualquier lugar del servidor necesitarás asegurar los permisos NTFS de todos los discos duros. Para hacer esto, primero tendrás que establecer los permisos para cada unidad.

Desde dentro de windows explorer, se debería hacer right click en la unidad c y seleccionar propiedades. Selecciona la pestña de ‘Seguridad’ y quita el usuario ‘Everyone’.



Repite el proceso para todas las unidades en el servidor.

Ahora necesitamos activar la cuenta de usuario 'FB_USER' dentro de la carpeta específica donde se requieren los permisos de acceso para leer y escribir. First of all, select the install folder for Firebird itself, right click the folder and select properties.



Añade la cuenta 'FB_USER' y asegura que se establecen los siguientes permisos:

- · Read & Execute
- · List Folder Contents
- · Read
- · Write

Repite este proceso para cada carpeta donde quieras que se localicen las Bases de Datos.

Nota: NTFS usa herencia para los permisos, así cada carpeta y archivo hereda los permisos de la carpeta donde se encuentran.

firebird.conf

FB puede ser más seguro mediante el uso del archivo firebird.conf. Cualquier cambio hecho a este archivo de configuración requiere que el Servicio de Firebird se reinicie antes de que los cambios tomen efecto.

Si no te sientes a gusto modificando el archivo firebird.conf puedes bajarte una utilidad de (http://prdownloads.sourceforge.net/firebird/FbConfigManager.zip) que se diseño para manipular el archivo.conf.

DB Paths/Directorios

Esta entrada se puede usar para restringir los paths que se pueden usar para guardar los archivos de las Bases de Datos. Son válidos los siguientes valores:

- · Full. Allows unlimited access to local drives.
- · Restrict. Restricts paths to specific list of paths.
- · None. Restricts to only those files listed in Aliases.conf.

Archivos externos Paths/Directorios

Define donde se guardan las tablas externas. Son válidos los siguientes valores:

- · Full. External tables can be stored anywhere on local drives.
- · Restrict. Restricts external table locations to a specified list of paths.
- · None. Does not allow external tables.

Por razones de seguridad, se recomienda que se especifique None.

Funciones Externas (UDF) Paths/Directorios

Define si las funciones definidas por el usuairo (UDF) se pueden localizar. UDF's son archivos tipo dll que se linkan dinámicamente en el proceso de FB en tiempo de ejecución. FB viene con una librería udf que se instala dentro $(FIREBIRD)\udf. Son válidos los siguiente valores:

- · Full. Las librerías UDF se pueden localizar en cualquier lugar dentro del disco local.
- · Restrict. Las librerías UDF se restringen a paths específicos.
- · None. No se permite el uso de librerías UDF.

Por seguridad se recomienda que uses Restrict seguido por UDF por ejemplo

UdfAccess = Restrict UDF

Esto permitirá a los usuarios tener acceso total a las librerías UDF estándares, pero no les permite upload sus propias librerías UDF.

TCP Protocol Settings

Define el puerto usado por FB para las comunicaciones TCP. FB1.5 introduce la posibilidad de configurar qué puerto se usa. El puerto por defecto es el 3050. Los siguientes valores son válidos cuando se cambia el puerto:

- RemoteServiceName = gds_db. Specifica el puerto dentro del Services File.
- RemoteServicePort = 3050. Se puede cambiar a cualquier puerto no usado.

Cambiando este valor se romperá la compatibilidad con vijos programas que no se configuran para usar puertos alternativos.

Remote Bind Address

Define que dirección IP se vinculada a FB. Por defecto, se vincula a todas las direcciones IP disponibles. Se puede establecer el siguiente valor:

- RemoteBindAddress = [IP ADDRESS]

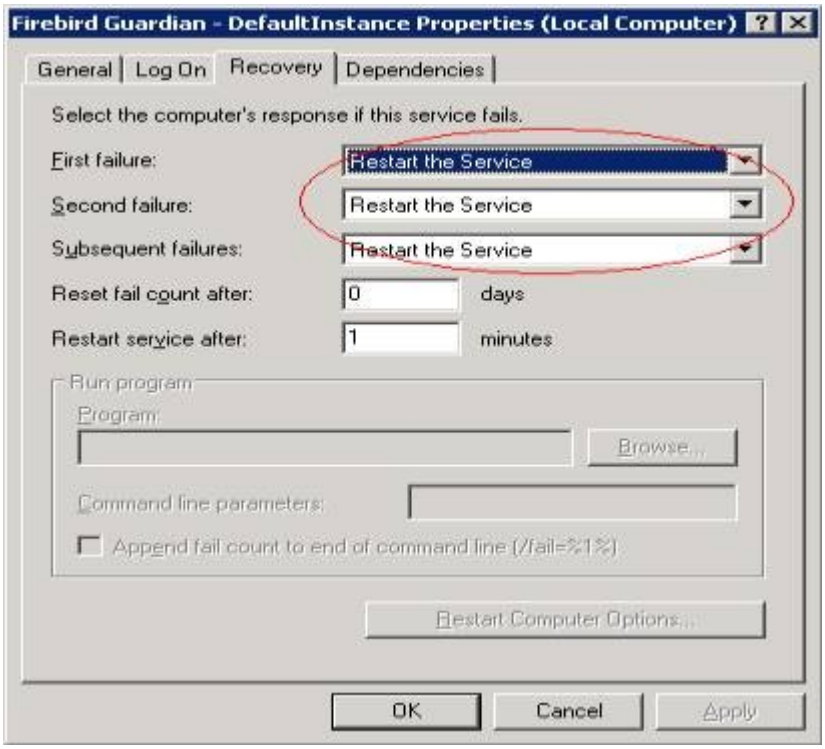
e.g. RemoteBindAddress = 192.168.0.1

La Remote Bind Address e útil cuando se instalan múltiples servidores FB, o cuando quieras controlar que interfaces se usan para las comunicaciones externas.

Propiedades de los Servicios

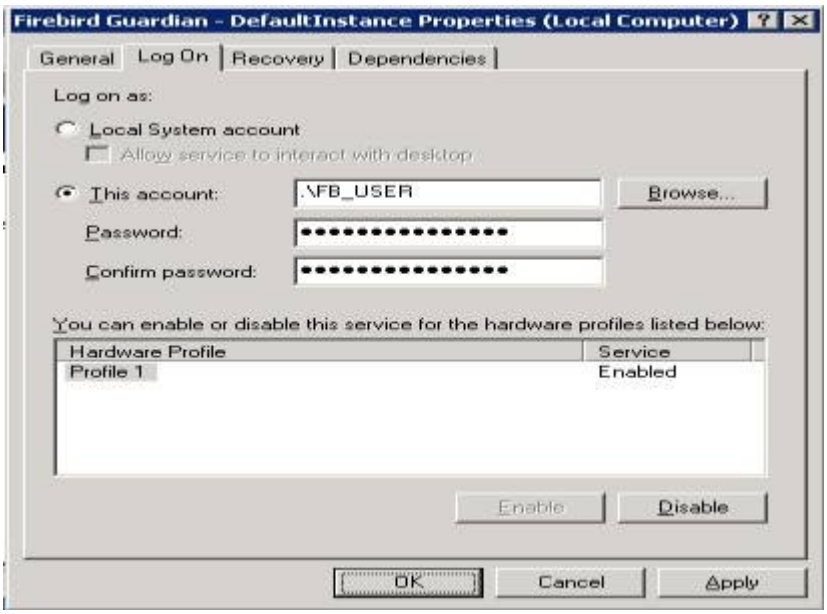
Por defecto Firebird se ejecuta como un Servicio dentro de Windows 2003, y viene con una aplicación de servicio Guardian para asegurar que siempre se está ejecutando. Sin embargo, un problema con el Guardian es que cuando el usuario que está ejecutando no tiene permisos para iniciar un servicio (como sucede en el contexto de la cuenta FB_USER que se ha creado previamente) entonces no funcionará. Para combatir esto necesitarás cambiar las propiedades para el Servicio FB.

Para cambiar las propiedades del Servicio 'Firebird Server – DefaultInstance' dentro del Services applet (Control Panel). Haz Doble click en el servicio para mostrar las propiedades y selecciona la pestaña de Recovery.

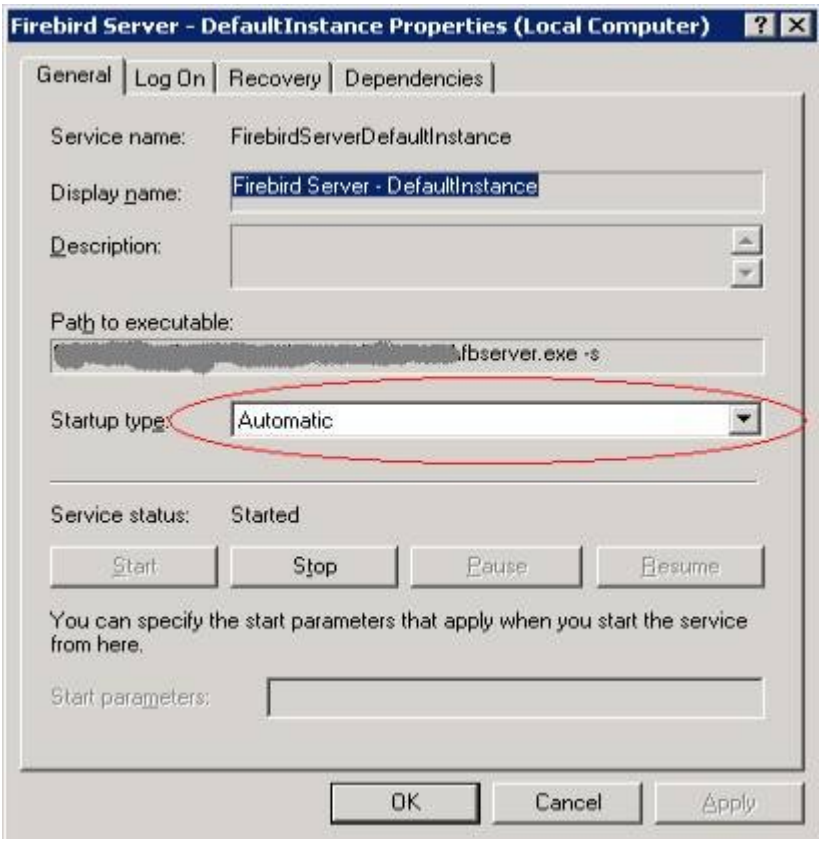


Asegura que las respuesta de error reinician el servicio (Restart the Service), como está indicado en la foto.

Ahora selecciona la pestaña de Log On y cambia el Log on para que se ejecute el servicio mediante el uso de la cuenta FB_USER que se ha creado previamente. Asegurate de que el password y el password de confirmación se establecen correctamente pues de otra forma el servicio no se iniciará..



A continuación cambia el tipo de Inicio dentro de la pestaña de General a Automático



Finalmente, haz click en OK para guardar los cambios y repite los pasos anteriores sobre el FB Guardian. Cuando estén completos restaura ambos servicios.

Archivos de Log

FB mantiene un archivo de log dentro de la carpeta FB_Install; esto se puede usar en conjunción con Windows Event Viewer para disgnosticar cualquier problema dentro del proceso de instalación.

Conclusion

Firebird debería ahora estar instalado de forma segura para su uso por los clientes.

Los siguientes links contienen información sobre Firebird y podría ser útil:

http://firebird.sourceforge.net/ff/foundation/ - Firebird foundation es una organización sin ánimo de lucro oriendtada al desarrollo y mejora de Firebird.

http://www.ibphoenix.com – IBPhoenix es una web y organización que facilita información recursos sobre Firebird.

http://www.volny.cz/iprenosil/interbase/ip_ib_isc4.htm - Security Enahanced users database.