



banckup

Manual de Usuario

Banckup On-line Backup Professional

Arnau Cabedo
Departamento Técnico
Banckup
febrero de 2010



Departamento de Formación y Soporte

Manual de Usuario: Banckup Online Backup Pro

febrero de 2010

Copyright © Data Copy Systems S.L.

Todos los derechos reservados. Queda prohibida la reproducción total o parcial de este documento en cualquier forma y por cualquier medio sin la autorización expresa del autor bajo pena de incurrir en la violación a los derechos de la propiedad intelectual.

Publicado por Banckup, febrero de 2010.

Edición 1.0

Autor: Banckup
Aplicación: Banckup Online Backup Pro
Versión: 5.5.5.0
Web: <http://www.banckup.net>

Esta edición aplica a la versión 5.5.5.0 de la aplicación cliente versión Profesional de Backup Online de Banckup.

Contenidos

1. INTRODUCCIÓN	6
2. REQUISITOS DEL SISTEMA.....	7
2.1. Equipo	7
2.2. Sistema Operativo.....	7
2.3. Comunicaciones.....	8
3. ¿CÓMO INSTALAR LA APLICACIÓN?.....	9
3.1. Instalación en Windows	9
3.2. Instalación en Linux	10
3.3. Instalación en Mac OS.....	10
4. ¿CÓMO EMPEZAR?.....	11
4.1. Primera ejecución.....	11
4.2. Acceso a la aplicación.....	12
4.3. Interfaz gráfica.....	12
5. ¿CÓMO REALIZAR UN BACKUP?	15
5.1. Crear un programado nuevo	15
5.2. Modificar un programado	26
5.3. Eliminar un programado.....	26
6. TIPO DE COPIAS DE SEGURIDAD.....	27
6.1. Lista de compatibilidades	27
6.2. Backup de ficheros/carpetas comunes.....	28
6.3. Backup de Oracle.....	28
6.4. Backup de bases de datos Microsoft SQL	29
6.5. Backup de Lotus Domino y Notes	31
6.6. Backup de Microsoft Exchange Server	31
6.7. Backup de Windows System State.....	33
6.8. Backup de bases de datos MySQL	34
7. ¿CÓMO RECUPERAR UN FICHERO?	36
7.1. Recuperación de ficheros/carpetas comunes	36
7.2. Recuperación de una base de datos Oracle	36
7.3. Recuperación de bases de datos Microsoft SQL.....	37

7.4. Recuperación de Lotus Domino y Notes	37
7.5. Recuperación de Microsoft Exchange Server	37
7.6. Recuperación de Windows System State	37
7.7. Recuperación de bases de datos MySQL	38
8. OTRAS CARACTERÍSTICAS.....	39
8.1. Primera copia	39
8.2. Tecnología In-File Delta	39
9. ¿CÓMO DESINSTALAR LA APLICACIÓN?	44
9.1. Desinstalación en Windows	44
9.2. Desinstalación en Linux	44
9.3. Desinstalación en MAC OS	44
10. GLOSARIO	45
10.1. Copia de seguridad	45
10.2. Backup	45
10.3. Copia de seguridad remota	45
10.4. Copia de seguridad local	45
10.5. Backup on-line	45
10.6. Servidor remoto.....	45
10.7. Datacenter.....	45
10.8. Unidad de almacenamiento local	46
10.9. Cifrado (“ <i>Encriptación</i> ”).....	46
10.10. Compresión.....	46
10.11. Nombre de usuario	46
10.12. Password.....	46
10.13. Frase o Clave de cifrado.....	46
10.14. Primera copia.....	47
10.15. Copia local	47

1. Introducción

Banckup Online Backup **Pro** es una solución de copias de seguridad remotas diseñada para proporcionar una aplicación robusta y fiable pero de fácil uso para la protección de sus datos más valiosos contra robos o pérdidas de información, fallos de disco, fuego y otros desastres inesperados.

Con Banckup Online Backup **Pro** se puede copiar todo tipo de información: documentos, fotografías, música, vídeos, correo electrónico, etc. Además, en su versión profesional, permite una alta disponibilidad de las aplicaciones empresariales, proporcionando un alto nivel de protección de datos gracias a una tecnología que permite mejorar significativamente el rendimiento y la utilización de los recursos disponibles. Además, cuenta con módulos para posibilitar la copia de correo, bases de datos y servidores de aplicaciones sin necesidad de tener que apagar estos servicios para ello.

Este manual contiene información acerca de cómo instalar, configurar, mantener y usar la aplicación Profesional de Backup Online de Banckup.

2. Requisitos del sistema

2.1. Equipo

La aplicación de backup online de Banckup se ha diseñado para no sobrecargar el equipo en ningún aspecto, por lo que los requisitos para que funcione correctamente son perfectamente asumibles por la mayoría de ordenadores de hoy en día. La tabla que se muestra a continuación recoge las características mínimas que su equipo debe tener.

Componente	Mínimos recomendados
CPU	Pentium II a 166MHz o superior
Memoria RAM	128MB (256MB recomendados)
Espacio en disco	110MB
Conexión a Internet	Conexión ADSL o superior

2.2. Sistema Operativo

Banckup Online Backup Pro está desarrollado en Java, con lo que es compatible con todos los sistemas operativos más comunes:



- Microsoft Windows 2000 Professional / Server / Advanced Server (32 bits)
- Microsoft Windows 2000 Datacenter Server (32 bits)
- Microsoft Windows 2003 Standard / Enterprise / Datacenter (32 / 64 bits)
- Microsoft Windows 2003 R2 Standard / Enterprise / Datacenter (32 / 64 bits)
- Microsoft Windows 2008 Standard / Enterprise / Datacenter (32 / 64 bits)
- Microsoft Windows XP Home / Professional (32 / 64 bits)
- Microsoft Windows Vista Home / Business / Ultimate (32 / 64 bits)
- Microsoft Windows 7 Home Premium / Professional / Ultimate (32 / 64 bits)
- Mac OS X v10.3 Panther (Java 1.4.2 support v10.3.4 or later)
- Mac OS X v10.4 Tiger
- Mac OS X v10.5 Leopard
- Mac OS X v10.6 Snow Leopard
- Red Hat Enterprise Linux 3 (32 / 64 bits)
- Red Hat Enterprise Linux 4 (32 / 64 bits)
- Red Hat Enterprise Linux 5 (32 / 64 bits)
- CentoOS 3 (32 / 64 bits)

- CentoOS 4 (32 / 64 bits)
- CentoOS 5 (32 / 64 bits)
- Solaris 10 (x86)
- FreeBSD 6.4 (32 / 64 bits)
- FreeBSD 7.1 (32 / 64 bits)

2.3. Comunicaciones

Banckup Online Backup Pro utiliza puertos estándar para la comunicación con el servidor, con lo que no requiere de configuración especial.

Si la aplicación no pudiera establecer conexión con el servidor remoto de backup, verifique que su firewall y/o antivirus no esté bloqueando la comunicación.

3. ¿Cómo instalar la aplicación?

En esta sección se explica cómo realizar la instalación de la aplicación de backup online de Banckup. Como podrá comprobar se trata de un proceso estándar muy sencillo que no le llevará más de unos pocos minutos.

NOTA: Para poder utilizar la aplicación de backup online, recuerde que debe estar registrado como usuario de Banckup. Para darse de alta en el servicio o si desea simplemente probarlo, puede dirigirse a <http://www.banckup.net>.

Para cualquier duda o consulta técnica, puede dirigirse a la sección de Soporte de la web de Banckup, donde encontrará tutoriales y guías de usuario.

<http://www.banckup.net/es/site/support>

3.1. Instalación en Windows

Si ya es usuario registrado de Banckup y todavía no dispone del instalador de la aplicación, puede descargárselo del siguiente enlace de Internet:

<http://www.banckup.net/site/downloads/obm-win.exe>

Una vez descargado el instalador (archivo .EXE), procederemos a ejecutarlo (doble clic sobre él):

- Seleccione el idioma a utilizar durante la instalación.
-
- Pinche en “Siguiente” en la pantalla de bienvenida para continuar.
- Acepte el acuerdo de licencia y pinche en “Siguiente” en la pantalla de bienvenida para continuar.
- Seleccione la carpeta donde guardar instalar la aplicación.
- Seleccione qué usuarios podrán utilizar la aplicación.
- Revise que la configuración sea correcta y pinche en “Instalar” para empezar.
- Una vez que el instalador haya acabado de copiar los datos, pinche en “Finalizar” para completar la instalación.
- Un acceso directo se ha creado en el escritorio de Windows y en la bandeja del sistema le aparecerá otro icono con el estado de la aplicación.

3.2. Instalación en Linux

Si ya es usuario registrado de Banckup y todavía no dispone del instalador de la aplicación, puede descargárselo del siguiente enlace de Internet:

<http://www.banckup.net/site/downloads/obm-nix.tar.gz>

Una vez descargado el instalador, siga el siguiente procedimiento:

- Descomprima el paquete en /usr/local/obm:

```
# mkdir /usr/local/obm  
# cd /usr/local/obm  
# gunzip obm-nix.tar.gz  
# tar -xf obm-nix.tar
```

- Ejecute el script de instalación:

```
# ./bin/install.sh > install.log
```

- Los servicios para la actualización y la ejecución programada de las copias de seguridad quedan instalados durante este proceso.
- Una vez finalizada la instalación, puede ejecutar la aplicación directamente desde el modo gráfico o habiendo habilitado el modo gráfico e introduciendo el siguiente comando:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

3.3. Instalación en Mac OS

Si ya es usuario registrado de Banckup y todavía no dispone del instalador de la aplicación, puede descargárselo del siguiente enlace de Internet:

<http://www.banckup.net/site/downloads/obm-mac.zip>

Una vez descargado el instalador, siga el siguiente procedimiento:

- Descomprima el paquete de instalación.
- Ejecute el asistente de instalación.
- Reinicie el ordenador para finalizar la aplicación.
- Un acceso directo se ha creado en el escritorio.

4. ¿Cómo empezar?

Recuerde que para poder empezar a utilizar la aplicación, debe ser usuario registrado de Banckup, disponiendo de su nombre de usuario y contraseña, y tener la aplicación instalada (véase sección 3).

NOTA: En caso de desconocer su nombre de usuario o contraseña, consulte en primera instancia el e-mail de alta que recibió tras darse de alta en el servicio. En caso de no haber recibido dicho correo o de no disponer de él, envíe un e-mail a sopORTE@banckup.com solicitando la información e indicando algún tipo de información identificativa.

4.1. Primera ejecución

La primera vez que arranque la aplicación, ésta le pedirá que introduzca la configuración de conexión al servidor de backup remoto a utilizar.

Servidor de respaldo

Deje la configuración que le aparece por defecto, ya que ese es el servidor que Banckup le ha asignado para almacenar sus copias.

Configuración del proxy

En caso de que usted utilice un proxy para acceder a Internet, introduzca aquí la configuración requerida.

Datos de usuario

Introducida la información de conexión, se debe introducir la información de usuario que Banckup le ha facilitado. Para ello, seleccione la opción “¿Ya es usuario?” que aparece en el margen inferior izquierdo de la ventanita.

Introduzca su nombre de usuario y contraseña para acceder a la interfaz gráfica de la aplicación.

NOTA: Si Banckup no le ha facilitado su nombre de usuario y contraseña, contacte con el departamento de soporte.

Una vez autenticado y con la interfaz gráfica abierta, la aplicación le ofrece crear un primer programado que, por defecto, llama “New Backup Set”. Tanto el nombre como toda la programación del programado propuesto, son personalizables (véase sección 5.1). Si no se quiere crear ningún programado todavía, seleccione “Cancelar”.

A partir de aquí, usted ya puede empezar a utilizar la aplicación para realizar y programar sus copias de seguridad. Consulte las secciones correspondientes de este manual para saber cómo proceder con las tareas más comunes.

4.2. Acceso a la aplicación

Una vez instalada la aplicación y configurada para realizar automáticamente las copias de seguridad, el acceso a la interfaz gráfica de la aplicación sólo es necesario para realizar cambios en la configuración o para recuperar datos del repositorio de copias. La ejecución de los programados se realiza, según la programación introducida (véase sección 5.1), en segundo plano.

El acceso a la aplicación puede realizarse mediante el acceso directo que aparece en la carpeta de aplicaciones de su sistema operativo o bien a través del icono que aparece en la bandeja del sistema, en el caso de Windows.

El acceso requiere de autenticación, por lo que debe introducir su nombre de usuario y contraseña (Fig. 1).

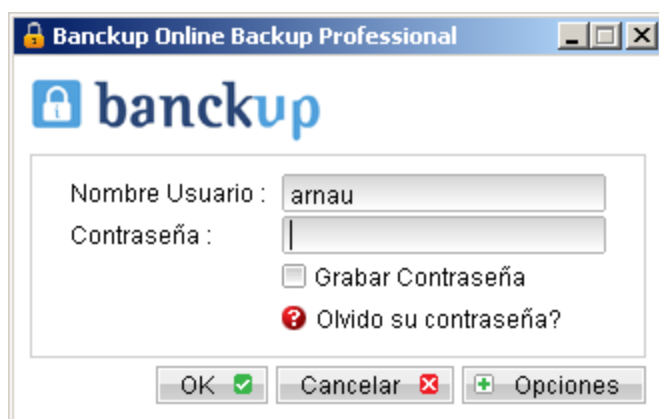


Fig. 1. Ventana de login.

4.3. Interfaz gráfica

Una vez autenticado, aparece la ventana que muestra la Fig. 2.

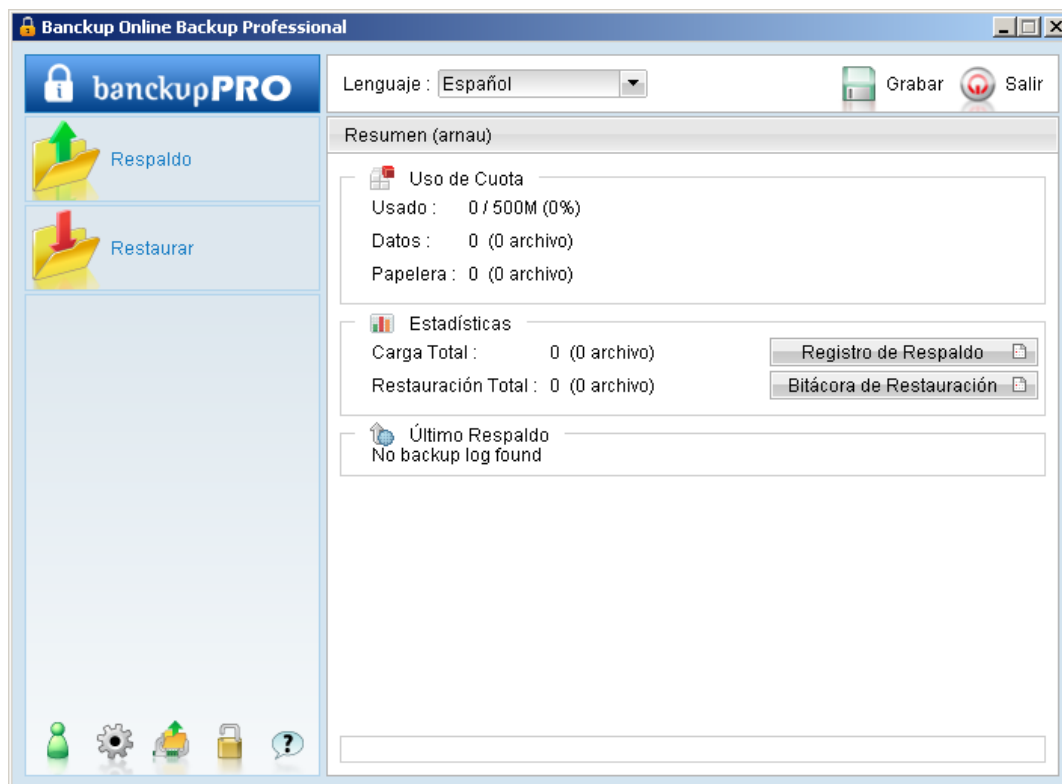







Fig. 2. Interfaz gráfica de la aplicación.

Tabla 1. Descripción de las opciones de la aplicación.

Opción	Descripción
Respaldo	Abre un menú desde el que se puede forzar el lanzamiento manual de una copia de seguridad previamente configurada.
Recuperar	Abre un menú desde el cual se puede recuperar la información del repositorio de sus copias de seguridad que se desee.
Lenguaje	Permite cambiar el idioma con que se muestra los textos de la interfaz gráfica. Hay más de 30 idiomas disponibles.
Grabar	Salva los cambios de configuración introducidos. Si se cierra la aplicación sin salvar, ésta le pregunta si desea hacerlo antes de salir.
Salir	Cierra la interfaz gráfica (las copias programadas se realizarán igualmente según programación establecida).
Perfil de usuario 	Abre una ventana desde la que se puede modificar la contraseña de usuario utilizada, cambiar el mail donde recibir los informes de backup, añadir otras direcciones de correo donde recibir los informes de backup y cambiar la zona horaria.
Ajuste de Respaldo	Opción desde la que se permite crear nuevos programados

	de copia de seguridad, modificar cualquier configuración de los ya creados y eliminar los que no se desee realizar más.
Decrypt Local Copy 	Asistente que permite la recuperación de ficheros de copias de seguridad locales, es decir, almacenadas en un dispositivo local o extraíble, no en el repositorio remoto de respaldo.
Descifrar ficheros 	Opción que permite descifrar archivos cifrados previamente por la aplicación.
Acerca de... 	Información acerca de la aplicación Banckup Online Backup Pro (versión, proveedor, contacto, etc.).
Registro de respaldo	Muestra información acerca de la realización y estado de sus copias de seguridad.
Bitácora de restauración	Muestra información acerca de la recuperación y estado de ficheros de su repositorio remoto.

5. ¿Cómo realizar un backup?

Banckup Online Backup Pro v.5.5.5.0 permite realizar copias de seguridad automáticas de, prácticamente, cualquier dato que usted pueda tener en su sistema.

Un programado de copia de seguridad contiene todos los ajustes de respaldo de una operación de copia de seguridad. Esta sección describe todas las prestaciones disponibles que se puede configurar en la definición de un programado de copias de seguridad y explica cómo puede utilizar cada una de ellas para llevar a cabo diferentes tareas.

Se puede definir tantos programados como se necesite. Cada uno de ellos es una entidad individual e independiente. Por ejemplo, si quiere que un directorio sea respaldado durante el día y que otro directorio sea respaldado durante la noche, puede crear dos programados, cada cual con la configuración deseada.

5.1. Crear un programado nuevo

Para crear un nuevo programado, simplemente haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +) y elija un tipo de datos a copiar.

Cuando se crea un programado se puede definir todas las características que a continuación se listan:

Tipo de ficheros a copiar

En función del tipo de fichero/datos a copiar, puede diferenciarse entre los siguientes tipos de copias de seguridad:

- ▶ Backup de ficheros/carpeta comunes
- ▶ Backup de Oracle
- ▶ Backup de bases de datos Microsoft SQL
- ▶ Backup de Lotus Domino y Notes
- ▶ Backup de Microsoft Exchange Server
- ▶ Backup de Windows System State
- ▶ Backup de bases de datos MySQL

Seleccione el que se adecúe al tipo de datos que desea proteger con copia de seguridad. En función de la opción elegida, la aplicación solicita una u otra información de configuración (véase sección 6).

Fuente de respaldo (datos a copiar)

La “fuente del respaldo” define qué datos han de incluirse en la realización de una copia de seguridad programada. Hay dos tipos de fuente de copia de seguridad: “Seleccionada”

y “No Seleccionada”. La fuente de respaldo “Seleccionada” define los archivos/directorios que deberán incluirse en el programado, mientras que la fuente de respaldo “No Seleccionada” define los ficheros/directorios que deben excluirse y, por lo tanto, no copiar.

La aplicación ofrece la posibilidad de configurar rápidamente la fuente de respaldo mediante una serie de “fuentes pre-definidas” (como la copia de los documentos personales del usuario, el correo, etc.). Para definir la fuente de respaldo de manera personalizada, pinche en “Configuración avanzada”.

NOTA: En sistemas operativos Microsoft Windows, si la opción “Ocultar los ficheros operativos protegidos (Recomendado)” está habilitada para el explorador de archivos, las carpetas/archivos del sistema no se mostrarán en la fuente de respaldo. Sin embargo, mediante la selección de las carpetas contenedoras de esos ficheros/carpetas, todos los subficheros (incluidos las carpetas/archivos del sistema), serán incluidos en la copia programada. Si quiere excluir archivos del sistema (como por ejemplo la papelera de reciclaje) de la copia de seguridad, debe seleccionar dichas carpetas/archivos directamente en vez de seleccionar la carpeta principal. Otra alternativa, es introducir la correspondiente ruta del sistema en la [Lista de Excluidos] del programado.

Unidad de red

Si necesita hacer una copia de seguridad de una unidad de red en Windows (sólo funcionará en Windows NT/2000/XP/2003), debe introducir su dominio de Windows, nombre de usuario y contraseña en la sección de [Recursos de Autenticación de Red para Windows] como se muestra abajo. Esto es necesario ya que el programa de copias de seguridad siempre se ejecutará bajo el contexto de la cuenta del “Sistema Local” de Windows (que no tiene los privilegios necesarios para acceder a los recursos de la red) por defecto. La aplicación necesita recoger su nombre de usuario de Windows, contraseña y nombre de dominio para autenticarse ante el controlador de dominios de Windows con el fin de adquirir los privilegios de acceso necesarios a los ficheros de la red que vayan a ser respaldos. Si no da su nombre de usuario ni contraseña, la aplicación tendrá problemas para acceder a los recursos de la red en su programa de tareas de copia de seguridad.

Si necesita hacer una copia de seguridad de una unidad de red en el programa de copias de seguridad, siga el siguiente procedimiento:

- 1) Seleccione el grupo de respaldo del panel de la izquierda y haga clic en el botón de [Propiedades].
- 2) Introduzca su dominio de Windows, nombre de usuario y contraseña en el recuadro que aparece abajo y haga clic en [OK].
- 3) Pulse en el botón de [Grabar] de la barra de herramientas.

Los pasos explicados anteriormente sólo son aplicables a ordenadores que funcionan en un dominio de Windows. Si no posee un dominio de Windows en su red y está utilizando un Grupo de Trabajo o un servidor de NetWare, por favor utilice el comando de “net use” para autenticar la ejecución del proceso de respaldo contra el equipo de la unidad de red.

De lo contrario, aparecerá el mensaje de error "Acceso Denegado" en el informe de copias de seguridad.

Por ejemplo, si quiere hacer una copia de seguridad de \\SERVER\SHARE que se encuentra en un servidor de NetWare (u otro ordenador del grupo de trabajo windows) y le aparece el mensaje de error "Network drive no es accesible", intente añadir el siguiente comando como un [comando Pre-backup].

```
net use \\SERVIDOR\SHARE [CONTRASEÑA] /USUARIO:[DOMINIO | MACHINE_NOMBRE]\[NOMBRE DE USUARIO]
```

Ejemplo:

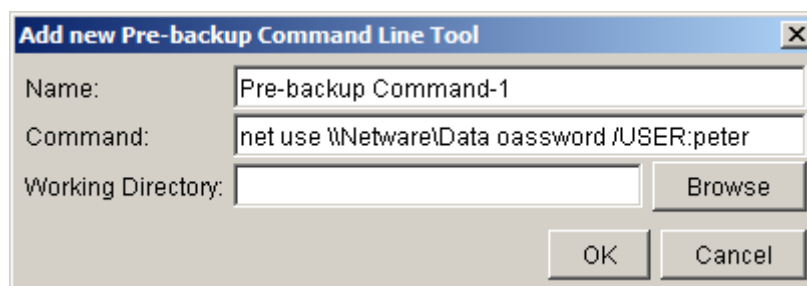


Fig. 3. Ejecución de un comando antes de la realización de la copia.

Introduzca uno de los siguientes comandos directamente en el Comando Pre-Backup:

```
net use \\Netware\Data password /USUARIO:peter
```

```
net use \\WorkgroupOrdenador1\Data password /USUARIO:WorkgroupOrdenador1\peter
```

Esto autenticará el proceso en curso con el servidor de NetWare (u otro ordenador en un grupo de trabajo de Windows) y la copia de seguridad se ejecutará correctamente.

Planificación de copias de seguridad

El programado puede configurarse para ser ejecutado cada cierto periodo de tiempo:

Tipo	Descripción
Diario	El programado se ejecuta diariamente.
Semanal	El programado se ejecuta el día o días de la semana que se especifique.
Mensual	El programado se ejecuta el día especificado o el día de mes que cumpla con la configuración especificada.
Personalizado	El programado se ejecuta una vez en la fecha especificada.

Para cada periodicidad de programación, las copias de seguridad se ejecutarán en el tiempo programado por un máximo de duración especificada (o hasta que toda la información haya sido respaldada si se elige la opción de [Parar una vez finalizada la

copia de seguridad]). Si una tarea de respaldo no termina dentro del periodo de duración máximo especificado, será interrumpida.

Es importante saber que se puede tener más de una programación dentro de cada grupo de respaldo. Por ejemplo, se puede tener un programa diario de respaldo que se ejecute a la 1:00 del mediodía y otro programa diario de respaldo que se ejecute a las 00:00 horas, a medianoche. La combinación de estos programas crea en efecto un programa de copias de seguridad que funciona diariamente a las 00:00 y a la 13:00 de cada día.

Filtro de ficheros

Un “Filtro de Copias de Seguridad” define las reglas de selección de archivos que permiten al usuario incluir/excluir fácilmente archivos a/del grupo de respaldo mediante la aplicación unos criterios definidos por el usuario a los nombres de los archivos o nombres de directorios.

Hay algunas reglas básicas en relación a los filtros de respaldo:

- Los filtros se comprueban en orden de creación. Una vez que se ha identificado la inclusión/exclusión, el resto de los filtros no se comprobarán.
- La inclusión/exclusión hecha por filtro siempre tiene prioridad sobre la selección de la fuente de respaldo.
- Si ninguno de los filtros se aplica a un archivo específico, éste será entonces comprobado por la selección de inclusión/exclusión de la fuente de respaldo.

Clave	Descripción
Nombre	Nombre del filtro
Directorio principal	El directorio principal al que se aplica el filtro. Las reglas de filtrado serán aplicadas a todos los archivos y/o directorios bajo este directorio.
Aplicar a	Define si se debe aplicar la regla de filtrado a los archivos y/o directorios
Correspondencia de patrón	Define las reglas de filtrado de un filtro. Una regla de filtrado puede ser de uno de los siguientes tipos: [Empieza con] Incluir/Excluir todos los ficheros/ directorios que comiencen con un nombre que siga cierto patrón. Por ejemplo: Puede usar B* para que encaje con todos los archivos cuyo nombre empiecen con la letra 'B' [Contiene] Incluir/Excluir todos los ficheros/ directorios cuyo nombre siga cierto patrón. Por ejemplo: Puede usar *B* para que encaje con todos los archivos cuyo nombre contenga la letra 'B' [Termina con] Incluir/Excluir todos los ficheros/ directorios

	<p>cuyo nombre termine siguiendo cierto patrón. Por ejemplo: Puede usar *.doc para que encaje con todos los archivos cuyo nombre termine en '.doc' (todos los documentos de Word)</p> <p>[Expresión] Incluir/Excluir todos los ficheros/ directorios cuyo nombre corresponda/ encaje una expresión frecuente.</p>
Modo de filtro	Define si quiere incluir o excluir los ficheros que coincidan en/del grupo de copias de seguridad. Además, para los archivos que no coincidan, puede elegir excluirlos (con el tipo de filtro incluir) o incluirlos (con el tipo de filtro excluir) dentro o fuera del serie/grupo de respaldo

Ejemplos:

Ejemplo 1: Si quiere solamente respaldar documentos de Word, Excel y PowerPoint en su directorio de documentos (ej. C:\Mis Documentos), debe configurar el filtro de copias de seguridad de la siguiente manera:

```

Directorio Superior = C:\Mis Documentos
Aplicar a = Fichero (seleccionado)
Correspondencia de Patrón = finaliza con
Patrón = *.doc, *.xls, *.ppt
Modo de Filtro = Incluir correspondencia
Excluir todos los otros = Sí
    
```

Ejemplo 2: Si quiere hacer copias de seguridad de todos los ficheros, excluyendo todos los *.exe, *.dll and *.tmp, en C:\Aplicaciones, debería programar su filtro de copia de seguridad del siguiente modo:

```

Directorio Principal = C:\Aplicaciones
Aplicar a = Fichero (seleccionado)
Correspondencia de Patrón = finaliza con
Patrón = *.exe,*.dll, *.tmp
Modo de Filtro = Excluir correspondencia
Incluir todos los otros = Sí
    
```

Ejemplo 3: Si ha hecho su selección de archivos (todos bajo C:\) del programa de la fuente de copias de seguridad pero quiere excluir todas las imágenes (por ejemplo *.jpg y *.gif) de su selección, debería programar el filtro de respaldo de la siguiente manera:

```

Directorio Principal = C:\ Aplicaciones
Aplicar a = Fichero (seleccionado)
Correspondencia de Patrón = finaliza con
Patrón = *.jpg, *.gif
Modo de Filtro = Excluir correspondencia
Incluir todos los otros = No
    
```

NOTA: La opción de [Incluir todos los otros] no está seleccionado porque no se quiere incluir todos los demás archivos (NO *.jpg, *.gif) bajo C:\ en el grupo de copias de seguridad.

Ejemplo 4 (Avanzado): Si quiere incluir todo, excepto el directorio de registro ["log"], bajo C:\Aplicaciones en un grupo de copias de seguridad, debe programar el filtro de respaldo de la siguiente manera:

```
Directorio Principal = C:\Aplicaciones
Aplicar a = Directory (seleccionado)
Correspondencia de Patrón = Expresión Regular
Patrón = ^log$
Modo de Filtro = Excluir correspondencia
Incluir todos los otros = Sí
```

Ejemplo 5 (Avanzado): Si quiere incluir todos los directorios llamados "log" de los ficheros del grupo de respaldo con un nombre de archivos que comience con "B" y termine en "*.doc" bajo C:\Mis Documentos en el grupo de respaldo, puede usar una expresión normal de "^B.*\doc\$" para llevar a cabo su selección. El filtro de respaldo puede establecerse entonces de la siguiente manera:

```
Directorio Principal = C:\Mis Documentos
Aplicar a = Fichero (seleccionado)
Correspondencia de Patrón = Expresión común
Patrón = ^B.*\doc$
Modo de Filtro = Incluir correspondencia
Excluir todos los otros = Sí
```

Pre/Post comandos

La función "Herramienta de Línea de Comando" tiene dos componentes principales, el comando [Pre-Respaldo] y el comando [Post-Respaldo]. Puede usar los comandos [Pre-Respaldo] o [Post-Respaldo] para ejecutar cualquier comando nativo del OS (sistema operativo) antes o después de ejecutar una tarea de copias de seguridad.

Directorio temporal

Si está ejecutando una tarea de copia de seguridad de un fichero con deltas habilitado o una tarea de respaldo tipo base de datos, la aplicación creará archivos temporales y el directorio que se utilizará para almacenar todos estos ficheros son definidos por [Configuración] -> [Directorio temporal para almacenar archivos de respaldo]. Para evitar problemas programe éste en una partición de disco que no sea de sistema que tenga suficiente espacio libre.

Puede programar el [Directorio temporal para almacenar los ficheros de copias de seguridad] en una unidad de red. Si elige esta opción, debe utilizar una ruta UNC (por ejemplo \\SERVIDORSHARE) y no se olvide de configurar el [Grupo de Respaldo] -> programa de [Recursos de Autenticación de Red para Windows].

Para conservar el uso de espacio de disco, puede programar la opción de [Eliminar archivos temporales tras el respaldo] para borrar los ficheros temporales automáticamente una vez que finalice la tarea de copia de seguridad.

Tamaño del bloque de transferencia

El tamaño del bloque de transferencia define el tamaño del bloque que la aplicación utilizará para transferir los bloques de respaldo. En general, las tareas de respaldo que usen un tamaño de bloque más grande tendrán un mejor funcionamiento, debido al menor número de conexiones que se realizan.

Sin embargo, algunos cortafuegos o servidores proxy pueden bloquear el tráfico saliente de la red (método HTTP/HTTPS POST) con un bloque de gran tamaño por razones de seguridad. Si está utilizando una red con este tipo de restricción, debe reducir el valor del tamaño de transferencia e intentarlo de nuevo.

Para cambiar el tamaño del bloque de transferencia de cualquier serie de copia de seguridad, seleccione el módulo de [Configuración] en el panel de la izquierda para que aparezca el panel de módulo [Configuración] a la derecha. Una vez hecho esto puede alterar el [Tamaño de Bloque de Transferencia]. Una vez haya hecho los cambios, sólo tiene que hacer clic en el botón de la barra [Grabar].

Vínculo Simbólico (sólo para Linux/Unix/Mac)

Bajo el sistema Unix/Linux/Mac, los usuarios pueden crear un vínculo simbólico para unir un fichero/directorio de otro directorio. Este programa define si quiere que la aplicación siga cualquier vínculo simbólico encontrado en su ruta de respaldo.

Para cambiar el seguimiento del vínculo simbólico de cualquier serie de copia de seguridad, debe seleccionar el módulo de [Configuración] en el panel de la izquierda para que aparezca el panel de [Configuración] a la derecha. Una vez hecho esto, puede hacer los cambios necesarios en [Seguir vínculo Simbólico]. Una vez haya hecho los cambios, sólo tiene que hacer clic en el botón de la barra que dice [Grabar].

Instantáneas de Volumen de Microsoft (VSS)

Instantáneas de Volumen de Microsoft (VSS) le permite hacer copias de seguridad de ficheros que están exclusivamente abiertas. Sin el VSS, le aparecerá el mensaje de error "El proceso no puede acceder al archivo porque otro proceso ha bloqueado una parte del fichero" si intenta hacer una copia de seguridad de un fichero que está abierto exclusivamente (por ejemplo el fichero Outlook PST).

NOTA: EL VSS solo está disponible en Windows XP / 2003 y debe tener privilegios administrativos para iniciar el servicio de VSS en un ordenador. Además, el VSS solo funcionará si al menos una de sus particiones está formateada utilizando NTFS.

Si está utilizando Windows 2003, debe instalar el parche de Windows 2003 VSS disponible en <http://support.microsoft.com/default.aspx?scid=kb:en-us:887827> antes de ejecutar el VSS.

Si se topa con algún problema cuando esté utilizando el VSS en Windows XP / 2003, la recomendación de Microsoft es que intente volver a registrarse en el servicio de Instantáneas de Volumen. Para ello, vuelva a ejecutar el guión de [Directorio de instalación de la aplicación]\bin\RegisterVSS.bat.

Si desea más información, por favor consulte la siguiente página que contiene una introducción de carácter técnico a los servicios de Instantáneas de Volumen (VSS):

<http://technet2.microsoft.com/windowsserver/en/library/2b0d2457-b7d8-42c3-b6c9-59c145b7765f1033.mspx>

Cifrado

Por defecto

Seleccione esta opción si desea utilizar la configuración preestablecida por la aplicación.

Personalizado

Seleccione esta opción si desea definir el algoritmo, modo y longitud del cifrado, así como la clave de cifrado.

También puede escoger la opción de no cifrar sus datos, con lo que la ejecución de las copias de seguridad será más rápida, sin embargo, esta opción no se recomienda por la falta de privacidad que ello puede suponer.

NOTA: El cifrado se define en el momento de crear el programado de copia de seguridad y por tanto no pueden ser modificados. Debe crear un nuevo programado si quiere cambiar los programas de codificación para una serie de respaldo.

Parámetro	Descripción
Algoritmo	<p>Define el algoritmo de codificación utilizado para codificar sus archivos de copias de seguridad. Hay tres algoritmos de codificación disponibles:</p> <p>[AES] Advanced Encryption Standard algorithm [DESede] Triple DES algorithm [Twofish] Twofish algorithm</p> <p>Le recomendamos que utilice el AES puesto que ha sido elegido como la codificación estándar para usos comerciales. Remítase a las referencias sobre Criptografía para más información sobre algoritmos de codificación.</p>
Modo	<p>Define el modo de codificación utilizado para codificar sus archivos de copias de seguridad. Hay dos modos de codificación disponible:</p> <p>[ECB] Electronic Cook Book Mode [CBC] Cipher Block Chaining Mode</p>

	Le recomendamos que utilice el modo CBC ya que ofrece mejor seguridad. Remítase a las referencias sobre Criptografía para más información sobre modos de codificación.
Clave	La clave utilizada para codificar todos los archivos dentro de una serie/ grupo de copias de seguridad.

NOTA: Guarde en lugar seguro su frase de cifrado, puesto que en caso de pérdida sus datos no podrán ser recuperados. Banckup **no** conoce su frase de cifrado, **sólo usted tiene acceso a sus datos copiados**. En caso de pérdida de la frase de cifrado, usted puede solicitar el reseteo de dicha frase enviando un e-mail a suporte@banckup.com, de manera que recuperará el acceso a su cuenta pero los datos no podrán ser recuperados, deberá realizar un backup completo de todos sus backup programados.

Política de retención

Durante el proceso de respaldo, si la aplicación encuentra que usted ha borrado un archivo (o lo ha actualizado) en su ordenador, guardará el archivo correspondiente borrado o actualizado ya respaldado en el servidor de copias de seguridad en una zona de retención del servidor de copias. El programa de política de retención define por cuánto tiempo se mantienen estos archivos en la zona de retención del servidor de copias de seguridad antes de que sean borrados automáticamente del mismo.

La política de retención únicamente afectará al archivo “retenido” (es decir, los archivos que ya han sido eliminados o actualizados en su ordenador y, por tanto, son trasladados a la zona de retención del servidor de copias de seguridad) Para aquellos archivos que no han sido actualizados en su ordenador, las copias de seguridad de los mismos se guardan en la zona de datos/ información del servidor de copias de seguridad y no se verán afectados por la política de retención. Estos archivos de respaldo de archivos no cambiados permanecerán en el servidor de copias de seguridad para siempre hasta que los archivos originales sean eliminados o actualizados desde su ordenador.

Política de Retención Estándar

La política de retención [Estándar] le permite borrar archivos retenidos automáticamente tras un número de días definido por el usuario o tras un número definido de tareas de respaldo. Para cambiar el programa de política de retención de cualquier serie de copia de seguridad, debe seleccionar el nódulo de [Política de Retención] en el panel de la izquierda. Hecho esto, puede hacer los cambios a su política de retención bajo la sección de [Política de Retención]. Una vez haya realizado los cambios, sólo tiene que hacer clic en el botón de la barra que dice [Grabar].

Política de Retención Avanzada

La política de retención [Avanzada] le permite configurar una política de retención más flexible. Le permite mantener/ guardar una serie de instantáneas de todos los ficheros respaldados basándose en el tiempo de las tareas de respaldo. Por ejemplo, puede configurar la política de retención avanzada para guardar las siguientes series de archivos

de copias de seguridad para imitar la antigua política de retención cuando se hacían rotaciones de cintas:

- ▶ Todos los archivos disponibles en los últimos 7 días
- ▶ Todos los archivos disponibles en los últimos 4 sábados de los últimos 28 días
- ▶ Todos los archivos disponibles el primer día de cada mes de los últimos 3 meses
- ▶ Todos los archivos disponibles el primer día de cada trimestre en los últimos 12 meses
- ▶ Todos los archivos disponibles el primer día de cada año en los últimos 7 años.

Para hacerlo, necesita programar la política de retención avanzada de la siguiente manera:

- ▶ Teclee = Diario; Número de copias a guardar = 7
- ▶ Teclee = Semanal; Frecuencia= Sábado; Número de copias a guardar = 4
- ▶ Teclee = Mensual; Frecuencia = Día 1; Número de copias a guardar = 3
- ▶ Teclee = Trimestral; Frecuencia = Día 1 of Jan, Apr, Jul, Oct; Número de copias a guardar = 4
- ▶ Teclee = Anual; Frecuencia = Fecha 01-01; Número de copias a guardar = 7

Asumiendo que hoy fuera 17-Enero-2006, si la opción [Elimine archivos retenidos por política de superposición] no está habilitada, un total de 22 instantáneas serán guardadas en el servidor de la siguiente manera (siempre que haya ejecutado las copias de seguridad a diario por más de 7 años):

Diariamente	Semanalmente	Mensualmente	Trimestralmente	Anualmente
16-Enero-2006	14-Enero-2006	01-Enero-2006	01-Enero-2006	01-Enero-2006
15-Enero-2006	07-Enero-2006	01-Dic-2005	01-Oct-2005	01-Enero-2005
14-Enero-2006	31-Dic-2005	01-Nov-2005	01-Jul-2005	01-Enero-2004
13-Enero-2006	24-Dic-2005		01-Abril-2005	01-Enero-2003
12-Enero-2006				01-Enero-2002
11-Enero-2006				01-Enero-2001
10-Enero-2006				01-Enero-2000

Si la opción [Elimine archivos retenidos por política de superposición] está activada, sólo las siguientes instantáneas son guardadas:

Diariamente	Semanalmente	Mensualmente	Trimestralmente	Anualmente
16-Enero-2006	14-Enero-2006	01-Enero-2006	01-Enero-2006	01-Enero-2006
15-Enero-2006	07-Enero-2006	01-Dic-2005	01-Oct-2005	01-Enero-2005
14-Enero-2006	31-Dic-2005	01-Nov-2005	01-Jul-2005	01-Enero-2004

13-Enero-2006	24-Dic-2005		01-Abril-2005	01-Enero-2003
12-Enero-2006				01-Enero-2002
11-Enero-2006				01-Enero-2001
10-Enero-2006				01-Enero-2000

La política semanal anula la política diaria de modo que los instantáneas del 10-Enero-2006, 11-Enero-2006, 12-Enero-2006, 13-Enero-2006 y 14-Enero-2006 son borrados. La política mensual anula la política semanal de modo que los instantáneas del 24-Diciembre-2005 y 31-Diciembre-2005 son borrados. La misma política se aplica mensual, trimestral y anualmente resultando en un total de 11 instantáneas.

Otras opciones

La copia de seguridad fuera de Línea está básicamente diseñada para usuarios de portátiles que están fuera de línea la mayor parte del tiempo y no pueden depender de que el programa de respaldo lleve a cabo dichas actividades de forma regular. El "Intervalo de Respaldo" permite a los usuarios de portátiles especificar el intervalo en el que les gustaría que su información fuera respaldada. Cuando el aparato esté online y este intervalo haya transcurrido la copia de seguridad se ejecutará automáticamente. Si se habilita "Habilitar Alerta de Respaldo", aparecerá un mensaje que pedirá al usuario que confirme el inicio de la copia de seguridad.

El programa de "Notificación de Email" es el número de días desde el último respaldo que hace que el servidor de copias de seguridad envíe una notificación de correo electrónico al cliente para recordarle que ejecute una copia de seguridad fuera de línea.

Cuando el programa de "Recordatorio de Backup al apagar el sistema" está habilitado, aparecerá un mensaje pidiendo al usuario que inicie una copia de seguridad antes de cerrar la sesión o apagar Windows.

Respaldo por Deltas

Véase la sección 8.2 para una descripción detallada sobre esta opción.

Copia local

Si quiere guardar una copia de seguridad extra de información en el disco duro local (además de una copia de seguridad de la información almacenada en el servidor) para minimizar el tiempo de restauración de ficheros y/o añadir una precaución extra de seguridad, puede hacer lo siguiente:

1. Seleccione la opción "Copia local" marcando el recuadro de esta opción.
2. Introduzca el directorio en el que desee guardar un backup extra de los archivos respaldados en el recuadro que aparece de [Copiar al Disco Duro Local].
3. Se guardará una copia extra de respaldo en el directorio de [Copiar al Disco Duro Local] cuando ejecute una tarea de respaldo.

Para la recuperación de los ficheros salvados en local, utilice la opción “*Decrypt Local Copy*” que se encuentra en la pantalla principal de la aplicación (véase sección 4.3).

5.2. Modificar un programado

Para modificar cualquier parámetro de configuración de un programado previamente creado, simplemente haga clic en el icono de “Ajuste de Respaldo”. Seleccione el parámetro que desea cambiar navegando por el menú de la izquierda y cambie la configuración en la parte central-derecha de la ventana abierta. Una vez finalizados todos los cambios, pulse en “Guardar”.

5.3. Eliminar un programado

Para eliminar un programado creado previamente, simplemente haga clic en el icono de “Ajuste de Respaldo” → seleccione el nombre del programado a eliminar de la lista desplegable → Eliminar (símbolo -).

Confirme la eliminación del programado respondiendo “S” a la pregunta de confirmación de eliminación.

6. Tipo de copias de seguridad

En función del tipo de fichero/datos a copiar, puede diferenciarse entre los siguientes tipos de copias de seguridad:

- Backup de ficheros/carpeta comunes
- Backup de Oracle
- Backup de bases de datos Microsoft SQL
- Backup de Lotus Domino y Notes
- Backup de Microsoft Exchange Server
- Backup de Windows System State
- Backup de bases de datos MySQL

6.1. Lista de compatibilidades

Banckup Online Backup Pro v.5.5.5.0 permite realizar copias de seguridad de todos aquellos archivos comunes que puedan hallarse en su ordenador (*.doc, *.xls, etc.).

La lista que a continuación se muestra recoge las versiones de terceras aplicaciones de las que se puede realizar backup en caliente (sin necesidad de apagar estas aplicaciones para realizar la copia de los ficheros con que trabajan éstas).

- ▶ Microsoft Exchange Server 2000 / 2003 / 2007
- ▶ Microsoft SQL Server 7.0 / 2000 / 2005 / 2008
- ▶ Lotus Domino / Lotus Notes 5.0 o superior
- ▶ Oracle 8i o superior
- ▶ MySQL 3.2.4 o superior
- ▶ Outlook / Outlook Express i.e. *.pst, *.dbx and *.wab
- ▶ Other common files e.g. *.doc, *.xls

También es posible la copia en caliente de:

- ▶ Windows System State (todas las versiones excepto Vista / Server 2008)
- ▶ Windows System Backup para Vista / Server 2008
- ▶ Windows NTFS access privileges
- ▶ Linux access privileges and modes
- ▶ Mac OS X metadata and resource forks

6.2. Backup de ficheros/carpetas comunes

Para crear un nuevo programado que realice una copia de seguridad de ficheros o carpetas comunes, siga el siguiente procedimiento:

1. Haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +).
2. Seleccione la opción “Ficheros/carpetas comunes”.
3. Introduzca un nombre para identificar el programado.
4. Seleccione los archivos/directorios de los que quiera tener copia de seguridad.
5. Establezca toda la configuración para el programado (véase sección 5.1).
6. Guarde el programado.

6.3. Backup de Oracle

Este capítulo describe detalladamente cómo configurar la aplicación para realizar copias en caliente de bases de datos Oracle 8i/9i.

Requisitos

- ▶ Debe instalarse la aplicación en el ordenador que pueda conectarse a su servidor de Oracle 8i/9i utilizando el protocolo TCP/IP.
- ▶ Los datos de la base de datos de Oracle 8i/9i serán respaldos en un directorio temporal antes de ser enviados al Servidor de copias de seguridad remoto. Asegúrese de que dispone de suficiente espacio en el ordenador para guardar esto datos cuando ejecute la tarea de respaldo.
- ▶ La Base de datos debe estar en el modo de *archived log*.

Vista General

- Conectar a la base de datos Oracle utilizando SQL*NET sobre TCP/IP.
- Ejecutar todos los Pre-Comandos de este serie de respaldo.
- Si el tipo de backup a ejecutar es [Tipo Base de datos Backup],
 - ▶ Todos los archivos de datos en cada uno de los *tablespace(s)* seleccionados son copiados al directorio temporal especificado por este grupo de backup.
 - ▶ Si hay archivos temporales en la base de datos, el guión para volver a crear los archivos temporales se genera en un archivo localizado en el directorio temporal especificado por este grupo de backup.
 - ▶ Todos los parámetros de inicialización que no sean por defecto serán transferidos a un archivo de inicialización localizado en un directorio temporal especificado por este grupo de backup.

- ▶ Todos los archivos de control serán copiados al directorio temporal especificado por este grupo de backup.
- ▶ Todos los archivos de registro archivados serán copiados al directorio temporal especificado por este grupo de backup.
- Si el tipo de respaldo a ejecutar es [Tipo Backup *Archive Log*],
 - ▶ Todos los ficheros de registro archivados serán copiados al directorio temporal especificado por este grupo de backup.
- Ejecutar todos los Post-Comandos de este grupo de respaldo.
- Cargar todos los ficheros copiados al directorio temporal en el Servidor de copias de seguridad remoto.
- Eliminar los archivos temporales del directorio temporal si está habilitado [Configuración] -> [Directorio temporal para guardar archivos respaldo].

Cómo hacer copias de seguridad de la base de datos Oracle

1. Haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +).
2. Seleccione la opción “Grupo de Respaldo ORACLE DATABASE”.
3. Introduzca un nombre para identificar el programado.
4. Introduzca la contraseña del sistema, el Anfitrión del Servidor de la Base de datos Oracle, Puerto y SID.
5. Seleccione el *tablespace(s)* que desee copiar.
6. Introduzca una localización temporal para guardar los ficheros de copias antes de mandarlos al servidor de copias de seguridad remoto.
7. Establezca la programación de copias de seguridad para el respaldo de la base de datos y el respaldo de los *archived logs*.
8. Establezca toda la configuración para el programado (véase sección 5.1).
9. Seleccione el tipo de copia de seguridad que desee realizar (por ejemplo Copia de seguridad de Base de datos, Copia de seguridad de *Archived Log*).
10. Guarde el programado.

6.4. Backup de bases de datos Microsoft SQL

Requisitos

- ▶ La aplicación debe instalarse en el ordenador o servidor que tenga instalado el Servidor Microsoft SQL.

- ▶ Los datos del Servidor Microsoft SQL serán respaldos en un directorio temporal antes de ser enviados al servidor de copias de seguridad remoto. Asegúrese de que dispone de suficiente espacio en el ordenador para guardar estos datos cuando ejecute la tarea de respaldo.

Vista General

La aplicación hará copias de seguridad de la(s) base(s) de datos de su Servidor Microsoft SQL siguiendo los siguientes pasos:

- Antes de ejecutar ninguna actividad de respaldo, la aplicación ejecutará todos los Comandos Pre-Respaldo del grupo de seguridad.
- Para cada Base de datos que deba copiarse, la aplicación emitirá un comando de registro de transacción de copia de seguridad/ base de datos al Servidor Microsoft SQL para que copie cada Base de datos en un fichero de copia de seguridad del Servidor Microsoft SQL (*.bak file) y lo guarde en el directorio temporal que haya especificado.
- Una vez que todos los ficheros *.bak hayan sido puestos en cola en los directorios temporales, la aplicación ejecutará todos los Comandos Post-Respaldo del grupo de copias de seguridad.
- Cargue todos los ficheros respaldos al directorio temporal en el servidor de copias de seguridad remoto.
- Borre los archivos temporales del directorio temporal si está habilitado [Configuración] → [Directorio Temporal para almacenar Archivos de Respaldo].

Cómo hacer copias de seguridad de la Base de datos del Servidor Microsoft SQL

1. Haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +).
2. Seleccione la opción “Grupo de Respaldo Servidor MS SQL”.
3. Introduzca un nombre para identificar el programado.
4. Introduzca el nombre de usuario y la contraseña del Servidor Microsoft SQL.
5. Seleccione la(s) base(s) de datos que desea copiar.
6. Introduzca una localización temporal para guardar los ficheros de copias antes de mandarlos al servidor de copias de seguridad remoto.
7. Establezca la programación de copias de seguridad para el respaldo de la base de datos completa y el respaldo de registro de transacciones.

8. Establezca toda la configuración para el programado (véase sección 5.1).
9. Seleccione el tipo de copia de seguridad que quiera realizar (por ejemplo Completa, Diferencial, Registro de Transacción).
10. Guarde el programado.

6.5. Backup de Lotus Domino y Notes

Documentación disponible en breve.

6.6. Backup de Microsoft Exchange Server

Este capítulo describe detalladamente cómo utilizar la aplicación para respaldar un Servidor Microsoft Exchange.

Requisitos

- ▶ Servidor Microsoft Exchange 2000 con Service Pack 3 y post-SP3 instalados. Remítase a <http://www.microsoft.com/exchange/> para más información. o Servidor Microsoft Exchange 2003.
- ▶ La aplicación debe ser instalada en el ordenador que tenga en funcionamiento el Servidor Microsoft Exchange 2000 / 2003.
- ▶ Los datos del Servidor Microsoft Exchange serán respaldados en un directorio temporal antes de ser enviados al Servidor de copias de seguridad remoto. Asegúrese de que tiene suficiente espacio en su ordenador para guardar estos datos cuando ejecute el programado.

Vista General

Un Servidor Microsoft Exchange 2000/2003 almacena los datos en un Directorio Activo de Windows así como en su base de datos. Para respaldar totalmente un servidor Microsoft Exchange 2000/2003, necesita respaldar los siguientes componentes:

- ▶ Windows System State
- ▶ Microsoft Information Store
- ▶ Microsoft Site Replication Service
- ▶ Microsoft Key Management Service (*Exchange 2000 solamente*)

La aplicación respaldará el servidor Microsoft Exchange siguiendo los siguientes pasos:

1. Ejecutar todos los Pre-Comandos de este grupo de respaldo.
2. Si el tipo de backup a ejecutar es [Tipo de Respaldo Base de datos],

- a) Windows System State será respaldado a un directorio temporal especificado en su programado.
 - b) Todas las bases de datos Exchange seleccionadas son respaldadas a un directorio temporal especificado en su programado.
3. Si el tipo de backup a ejecutar es [Tipo Registro de Transacción],
 - a) Los nuevos valores de registros de transacciones generados desde el último respaldo serán respaldos al directorio temporal
 4. Eliminar los valores de registro de transacción respaldados desde el Servidor Exchange.
 5. Ejecutar todos los Post-Comandos de este grupo de respaldo.
 6. Cargar todos los archivos de respaldo del directorio temporal a un servidor de copias de seguridad remoto.
 7. Eliminar los archivos temporales del directorio temporal si está habilitado [Configuración] → [Directorio temporal para almacenar archivos de respaldo].

Cómo hacer copias de seguridad de un servidor Microsoft Exchange

Siga las instrucciones siguientes para hacer copias de seguridad de su servidor Microsoft Exchange utilizando la aplicación:

1. Haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +).
2. Seleccione la opción “Grupo de Respaldo Servidor MS Exchange”.
3. Introduzca un nombre para identificar el programado.
4. Seleccione la base de datos que desea copiar.

NOTA: Si este servidor Exchange es también un controlador de dominio de este Directorio Activo, seleccione también la casilla de [System State]. O si no, instale la aplicación en el controlador de dominio de este Directorio Activo y seleccione la casilla de [System State] en ese ordenador.

5. Introduzca una localización temporal para guardar los ficheros de copias antes de mandarlos al servidor de copias de seguridad remoto.
6. Establezca la programación de copias de seguridad para el respaldo de la base de datos.
7. Establezca la programación de copias de seguridad para Respaldo Registro de Transacción.

- NOTA:** Puede tener más de una programación en un grupo de respaldo, es decir, puede llevar a cabo un respaldo de registro de transacción intra-día añadiendo más de una programación diaria de respaldo de registro de transacción a su grupo de respaldo).
8. Establezca toda la configuración para el programado (véase sección 5.1).
 9. Seleccione el tipo de copia de seguridad que quiera realizar (por ejemplo “Base de datos” o “Archivos de Registro”).
 10. Guarde el programado.

6.7. Backup de Windows System State

Esta sección describe detalladamente cómo utilizar la aplicación para respaldar Windows System State.

Requisitos

- ▶ Microsoft Windows XP Profesional / 2003
- ▶ La aplicación debe estar instalado en el ordenador que contenga el *system state* que quiera respaldar
- ▶ Windows *system state* será respaldado en un archivo temporal antes de ser enviado al servidor remoto de backup. Asegúrese de que dispone de suficiente espacio en su ordenador para guardar el archivo temporal cuando ejecute la tarea de respaldo.

Vista General

La aplicación respaldará el *System State* siguiendo estos pasos:

- ▶ Ejecutar todos los Pre-Comandos de este grupo de respaldo
- ▶ Windows *System State* será respaldado a un directorio temporal especificado en su serie de backup
- ▶ Ejecutar todos los Post-Comandos de esta serie de backup
- ▶ Cargar los archivos de respaldo de Windows *System State* del directorio temporal a un Servidor de copias de seguridad remoto
- ▶ Eliminar los archivos de respaldo temporales Windows *System State* del directorio temporal si se habilita [Configuración] → [Directorio temporal para almacenar archivos de respaldo]

Cómo hacer copias de seguridad del System State de Windows

Siga las instrucciones siguientes para hacer copias de seguridad de Windows *System State* utilizando la aplicación:

1. Haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +).
2. Seleccione la opción “Grupo de Respaldo del estado del sistema”.
3. Introduzca un nombre para identificar el programado.
4. Utilice el botón [*Cambiar*] para configurar el parámetro [Directorio temporal para almacenar archivos de respaldo] y marque [Eliminar archivos temporales después del respaldo] si quiere que los archivos temporales sean eliminados automáticamente tras el respaldo.
5. Introduzca una localización temporal para guardar los ficheros de copias antes de mandarlos al servidor de copias de seguridad remoto.
6. Establezca toda la configuración para el programado (véase sección 5.1).
7. Guarde el programado.

6.8. Backup de bases de datos MySQL

Este capítulo describe detalladamente cómo utilizar la aplicación para respaldar su servidor MySQL.

Requisitos

- ▶ La aplicación debe ser instalada en el ordenador que está usando el servidor MySQL.
- ▶ La información en el servidor MySQL será respaldada en un directorio temporal antes de ser enviada a un Servidor de copias de seguridad remoto. Asegúrese de que tiene suficiente espacio en su ordenador para guardar esta información cuando ejecute la tarea de respaldo.
- ▶ Debe haber una cuenta MySQL que pueda utilizarse para conectar desde el host local. Añada dos nuevas cuentas MySQL para el Backup Manager `mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' -> IDENTIFIED BY 'some_pass'; mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost.localdomain' -> IDENTIFIED BY 'some_pass'; mysql> FLUSH PRIVILEGES;` Son cuentas de superusuarios con todos los privilegios para poder hacer lo que sea con una contraseña de *some_pass*.

Vista general

La aplicación respaldará su servidor MySQL siguiendo estos pasos:

1. Ejecutar todos los Pre-Comandos de este grupo de respaldo (backup).
2. Todas las bases de datos (bien locales o externas seleccionadas son respaldadas en un directorio temporal especificado en este grupo de backup).

3. Ejecutar todos los Post-Comandos de este grupo de respaldo.
4. Cargar todos los archivos del directorio temporal a un servidor de copias de seguridad remoto.
5. Eliminar los archivos temporales del directorio temporal si está habilitado [Configuración] → [Directorio temporal para almacenar Archivos de respaldo]

Cómo hacer copias de seguridad de una base de datos MySQL

Siga las instrucciones siguientes para respaldar su Servidor MySQL utilizando la aplicación:

1. Haga clic en el icono de “Ajuste de Respaldo” → Nuevo (símbolo +).
2. Seleccione la opción “Grupo de Respaldo Servidor MySQL”.
3. Introduzca un nombre para identificar el programado.
4. Introduzca la contraseña raíz, el número de puerto TCP/IP del servidor MySQL y la ruta a la prestación de respaldo de MySQL (*mysqldump*).
5. Seleccione la(s) base(s) de datos que desea copiar.
6. Introduzca una localización temporal para guardar los ficheros de copias antes de mandarlos al servidor de copias de seguridad remoto.
7. Establezca la programación de copias de seguridad para el respaldo de la base de datos
8. Establezca toda la configuración para el programado (véase sección 5.1).
9. Guarde el programado.

7. ¿Cómo recuperar un fichero?

Para recuperar un fichero del que previamente se hizo copia de seguridad, el usuario debe seguir uno de los siguientes procedimientos, en función del tipo de información salvada.

7.1. Recuperación de ficheros/carpetas comunes

Recuperación desde repositorio remoto (servidor de respaldo)

Desde la interfaz gráfica de la aplicación, seleccione la opción “Recuperar” e indique el programado que salvó la información que ahora quiere recuperar.

Le aparecerán las carpetas y ficheros salvados. Explore y seleccione aquella información que quiera recuperar.

Recuperación desde repositorio local (disco duro local)

Si la copia de seguridad la realizó contra un disco duro local, puede recuperar la información siguiendo el siguiente procedimiento:

1. Pinche en la opción “Asistente de descifrado de archivos” que aparece en la interfaz gráfica de la aplicación.
2. Utilice el botón de [Mostrar] para localizar el directorio con los ficheros que quiere recuperar.
3. Si quiere ver diferentes versiones de todos los ficheros (mostrados en gris abajo), simplemente elija el botón de [Mostrar todos los archivos] en la ventana que se le ha abierto.
4. Introduzca el directorio en el que quiera que los ficheros de respaldo sean recuperados.
5. Pinche en el botón “Iniciar” para proceder a la recuperación de los ficheros.

7.2. Recuperación de una base de datos Oracle

Los ficheros de control, los ficheros de datos y los *archived logs* se guardan en el servidor de copias de seguridad remoto junto con la información completa de su ruta. Sólo tiene que volver a poner todos estos archivos en su localización original cuando lleve a cabo la restauración de una base de datos.

Para recuperar una base de datos Oracle, siga el siguiente procedimiento:

1. Recupere los archivos de backup de la base de datos Oracle que quiera recuperar (véase sección 7.1).
2. Vuelva a poner todos los ficheros de datos en su localización original.

3. Siga los procedimientos recomendados por Oracle o por su administrador de sistemas informáticos para proceder a la restauración de la base de datos.

7.3. Recuperación de bases de datos Microsoft SQL

Para recuperar una base de datos Microsoft SQL, siga el siguiente procedimiento:

1. Recupere los archivos de backup (.bak) de la base de datos SQL que quiera recuperar (véase sección 7.1).
2. Abra el administrador del servidor Microsoft SQL.
3. Siga los procedimientos recomendados por Microsoft o por su administrador de sistemas informáticos para proceder a la restauración de la base de datos.

7.4. Recuperación de Lotus Domino y Notes

Para recuperar los datos de un servidor Lotus Domino o Lotus Notes, siga el siguiente procedimiento:

Documentación disponible en breve.

7.5. Recuperación de Microsoft Exchange Server

Para recuperar la base de datos de un servidor Microsoft Exchange, siga el siguiente procedimiento:

1. Recupere los archivos de backup de Microsoft Exchange del servidor de copias de seguridad (véase sección 7.1).
2. Utilice la aplicación "ExchangeRestore.exe" (que incorpora el propio Microsoft Exchange) para restaurar el servidor de correo.
3. Siga los procedimientos recomendados por Microsoft o por su administrador de sistemas informáticos para proceder a la restauración de la base de datos.

7.6. Recuperación de Windows System State

Para recuperar el *System State* de Windows, siga el siguiente procedimiento:

1. Recupere el archivo de backup del *System State* (esto es, *SystemState.bkf*) del servidor de copias de seguridad (véase sección 7.1).
2. Utilice la aplicación "NTBackup.exe" (que incorpora el propio sistema operativo Windows) para restaurar su Windows System State.

3. Siga los procedimientos recomendados por Microsoft o por su administrador de sistemas informáticos para proceder a la restauración de la base de datos.

7.7. Recuperación de bases de datos MySQL

Para recuperar una base de datos Microsoft SQL, siga el siguiente procedimiento:

1. Recupere los archivos de backup (.sql) de la base de datos MySQL que quiera recuperar (véase sección 7.1).
2. Abra el administrador del servidor MySQL.
3. Siga los procedimientos recomendados por *Sun Microsystems/Oracle* o por su administrador de sistemas informáticos para proceder a la restauración de la base de datos.

8. Otras características

8.1. Primera copia

Si tiene mucha información (por ejemplo: 300GB) de la cual realizar copia de seguridad, tardará bastante tiempo en realizar por completo la primera copia de seguridad a través de Internet. Si se topa con este problema, puede utilizar la opción de “Primera copia” para hacer la primera copia en un disco duro extraíble (en vez de hacerlo directamente en el servidor) y luego hacer llegar el disco a Banckup por correo ordinario o servicio de mensajería postal, para que sea éste el que se encargue de hacer directamente el volcado de información al servidor de copias de seguridad.

Este proceso permite ahorrar días (e incluso semanas) en la realización de su primera copia de seguridad íntegra. Dado que las ejecuciones siguientes serán incrementales (solamente archivos nuevos o actualizados serán cargados en el servidor) no tendrá problema alguno cargando la información de seguridad posteriormente.

NOTA: Antes de utilizar esta opción, contacte con el distribuidor de su servicio de copias de seguridad y consulte las condiciones sujetas a esta opción.

Para realizar la “Primera copia” a un disco duro extraíble, haga lo siguiente:

1. Cree un programado nuevo (véase sección 5.1).
2. Como destino de la copia, seleccione “Disco duro local”.
3. Indique la carpeta donde guardar la copia.

Asegúrese de que tiene suficiente espacio libre en el directorio especificado.

8.2. Tecnología In-File Delta

Este capítulo describe en qué consiste la tecnología in-file delta y cómo in-file delta puede usarse para hacer copias de seguridad de grandes ficheros de bases de datos (por ejemplo un fichero 10GB Outlook.pst) sin tener que transferir todo el archivo de base de datos diariamente.

Vista General

La tecnología in-file delta es un algoritmo avanzado de bloques de datos que tiene la inteligencia de detectar cambios (delta) en el contenido del fichero entre dos ficheros. Utilizando este algoritmo, la copia de seguridad diaria de grandes archivos (por ejemplo un archivo 10GB Outlook.pst) a través de una conexión de internet de baja velocidad se hace posible porque únicamente requiere los cambios de información (que deberían ser marginales) desde la última vez que se hizo una copia de seguridad enviada a través de una conexión a internet de baja velocidad para completar la copia de un archivo grande

(asumiendo que la copia completa del archivo ha sido guardada ya en el servidor de copias de seguridad).

Este es el proceso que tiene lugar en la copia de seguridad de un archivo 10GB Outlook.pst cuando es respaldado por la aplicación con la tecnología delta in-file.

- Todos los archivos (10GB), junto con su fichero *checksum*, son respaldos en el servidor de copias de seguridad. Esto puede realizarse directamente a través de internet o indirectamente utilizando la prestación de carga de semilla en un disco duro extraíble.
- Cuando la copia de seguridad se ejecuta de nuevo más tarde (normalmente al día siguiente), la aplicación descargará la lista *checksum* de todos los bloques de datos de la copia de seguridad completa del archivo (o el último archivo de respaldo incremental) del servidor de copias de seguridad y lo usará para detectar todos cambios que hayan sido hechos en el archivo de Outlook.pst.
- Los cambios detectados serán entonces guardados en un archivo delta que será transferido al servidor de copias de seguridad. Se generará un nuevo fichero *checksum* que también será transferido. (Se asume que este archivo delta será pequeño puesto que el contenido de los archivos PST no cambia mucho durante el uso diario)
- Las copias de seguridad posteriores de este archivo 10GB Outlook.pst pasarán por las dos etapas anteriores de nuevo. Como se ha explicado, sólo un archivo delta pequeño y un archivo *checksum* serán transferidos al servidor de copias de seguridad.
- Ahora con la tecnología in-file delta, ya es posible la copia de seguridad diaria de grandes archivos a través de una conexión a internet de baja velocidad.

Tipo incremental delta in-file

El Delta Incremental facilitará que las copias de seguridad se realicen sin problemas. El delta se genera comparando con la última transferencia completa o archivo delta. El archivo delta generado es del mínimo tamaño posible y utiliza el mínimo ancho de banda durante el proceso de respaldo. Para restaurarlo, el archivo completo y todos los archivos delta hasta el momento determinado son necesarios para restaurar el archivo a un momento específico.

Ejemplo: Si diariamente añade unos cambios equivalentes a 100MB a un archivo de 10G Outlook.pst.

Tras la primera carga completa de una copia de seguridad, la aplicación continuará generando y transfiriendo archivos delta en vez de transferir el archivo completo hasta que se cumpla una de las siguientes reglas:

- a) El número de deltas generados desde la última copia de seguridad completa es mayor que la configuración [Número de Delta].
- b) El índice delta (la relación del tamaño del archivo delta en proporción al tamaño completo del archivo) es mayor que la configuración [Razón de Delta].

Utilizando el delta incremental, el delta generado al comparar el archivo actual con la última carga completa o archivo delta es de unos 100MB.

Puesto que el tamaño del archivo delta es de unos 100MB diarios, el índice delta (alrededor de 1%) impedirá que se haga una carga completa del archivo. En vez de eso, la aplicación continuará generando y cargando archivos delta hasta el día 102 (asumiendo que la carga del archivo completo se hiciera en el primer día) que es cuando el número de deltas generados excederá la configuración de [Número de Delta] y desencadenará la carga/ transferencia del archivo completo Outlook.pst. Se puede inhabilitar el [Número de Delta] y la [Razón de Delta] si no quiere cargar el archivo completo.

Todos los archivos delta se generan con respecto a los cambios hechos desde la última copia de seguridad incremental o total. Esto significa que el último archivo de respaldo completo y **TODOS** los archivos de respaldos incrementales delta son necesarios para restaurar la última instantánea de un archivo de copia de seguridad.

Tipo diferencial in-file delta

El Diferencial Delta facilitará que la recuperación se realice sin problemas. El delta es generado al comparar con el último archivo completo cargado. El archivo delta generado aumenta diariamente y utiliza más ancho de banda durante el proceso de respaldo. Para restaurarlo, el archivo completo y un solo archivo delta son necesarios para restaurar el archivo a un momento específico.

Ejemplo: Si diariamente añade unos cambios equivalentes a 100MB a un archivo de 10G Outlook.pst.

Tras la primera copia de seguridad completa, la aplicación continuará generando y transfiriendo archivos delta en vez de transferir el archivo completo hasta que se cumpla una de las siguientes reglas:

- a) El número de deltas generados desde la última copia de seguridad completa es mayor que la configuración [Número de Delta].
- b) El índice delta (la relación del tamaño del archivo delta en proporción al tamaño completo del archivo) es mayor que la configuración [Razón de Delta].

Utilizando el delta diferencial, el delta generado al comparar el archivo actual con la última carga completa o archivo delta es de unos 100MB para el 1^{er} delta, 200MB para el 2^o delta, 300MB 3^{er} delta y así sucesivamente.

Puesto que el archivo delta aumenta unos 100MB diariamente, el índice delta para el día 52 (el tamaño del archivo delta es aproximadamente $51 \times 100 = 5.1\text{GB}$, asumiendo que el archivo completo se cargó en el día 1) será superior al 50% excediendo la configuración del [Razón de Delta] lo que provocará que se cargue el archivo completo de Outlook.pst. Se puede inhabilitar el [Número de Delta] y el [Razón de Delta] si no quiere cargar el archivo completo.

Todos los archivos delta se generan con respecto a los cambios hechos desde la última copia de seguridad total (es decir, una copia de seguridad diferencial) Esto significa que

solamente el último archivo de copia de seguridad completa y el último archivo delta son necesarios para restaurar/restituir la última instantánea de un archivo de copia de seguridad. Esto significa que otros archivos intermedios son sólo necesarios si quiere restaurar otras instantáneas de un fichero de seguridad.

La copia de seguridad diferencial delta in-file tiene las ventajas de que un archivo delta corrupto sólo haría una versión particular de un archivo de seguridad no recuperable mientras que el resto de las copias de seguridad creadas por otros archivos delta de la misma carpeta quedarían intactas.

Tamaño de Bloque

El tamaño de bloque define el tamaño del bloque de datos que se utiliza para detectar los cambios entre la última copia completa o archivo de copia de seguridad delta y el archivo que se encuentra en el ordenador local en este momento. En general, cuanto más pequeño sea el tamaño del bloque, mayores son las probabilidades de encontrar entre el archivo de la última copia de seguridad y el archivo que se encuentra en el ordenador local un bloque de datos que sea idéntico. Por lo tanto, produce un archivo delta más pequeño pero requerirá más capacidad de procesamiento detectar estos cambios. Por otro lado, la copia de seguridad delta in-file funcionando con un tamaño de bloque más grande se ejecutará más rápidamente pero esto por lo general producirá un archivo delta de mayor tamaño.

En la mayoría de los casos, la configuración por defecto [Auto] elegirá por usted el tamaño de bloque óptimo para cada archivo (dependiendo del tamaño del mismo).

Tamaño Mínimo de Archivo

La configuración de [Tamaño Mínimo de Archivo] define el tamaño mínimo de archivo que éste debe tener antes de poder usar y aplicarse la tecnología delta in-file de copias de seguridad.

Si el tamaño de un archivo que está siendo respaldo es más pequeño que la configuración de [Tamaño Mínimo de Archivo], la tecnología delta in-file de copias de seguridad no se aplicará a este fichero, y todo el archivo, en vez de únicamente el archivo delta, será cargado en el servidor de copias de seguridad. No es necesario realizar copias de seguridad delta in-file en todos los ficheros porque respaldar todo un archivo no tarda tanto tiempo de todas maneras. En cambio, respaldar todo el archivo reduce la cantidad de tiempo necesaria para restaurar un archivo de respaldo.

Cargar un fichero completo de Nuevo

Número de Delta

La configuración de [No. de delta] define el máximo número de archivos delta procedentes del mismo fichero de copia de seguridad completa que se deberán generar y transferir al servidor de copias de seguridad antes de que un respaldo completo (todo el archivo) de este fichero sea cargado en el servidor de copias de seguridad.

Por ejemplo, si ya ha creado 100 archivos delta del archivo de copia de seguridad completa y la configuración de [No. de delta] está ajustada/ programada a 100, la próxima copia de seguridad realizara una carga todo el archivo completo en vez de solamente el archivo delta. Sin embargo, si la regla de [No. de delta] no está habilitada, seguirá generando archivos delta y cargándolos en el servidor de copias de seguridad hasta que la otra regla delta haga necesaria un respaldo completo (es decir, se exceda el índice delta). Esta configuración existe para asegurar que siempre habrá un fichero de respaldo completo después de que se hayan generado un cierto número de archivos delta

Razón de Delta

La configuración de [Razón de Delta] se define como el tamaño de un archivo delta dividido por el tamaño del fichero de copia de seguridad completa (es decir, el porcentaje de cambios detectados entre el fichero de la última copia de seguridad completa y el actual)

Si el índice delta calculado entre el tamaño del archivo delta generado y el tamaño del fichero de copia de seguridad completa es mayor que la configuración del [Razón de Delta], todo el fichero, en vez de únicamente el archivo delta, será respaldado en el servidor de copias de seguridad. Esto es así porque la diferencia entre copiar todo el fichero y el archivo delta no es significativa y, en cambio, resulta mejor cargar todo el fichero para reducir el tiempo necesario para restaurar el archivo.

La configuración por defecto de [Razón de Delta] es 50%. Esto significa que si un fichero cambia más de un 50%, todo el fichero, en vez de únicamente el archivo delta, será respaldado y cargado en el servidor de copias de seguridad.

Tipo delta In-file Avanzado

La configuración [Respaldo por deltas] → [Avanzado] permite a los usuarios anular el tipo delta in-file por defecto a un determinado número de días (por ejemplo todos los domingos o el primero de cada mes). Esto resulta útil si quiere todos los archivos de copias de seguridad delta in-file sean incrementales pero quiere también realizar un respaldo delta in-file diferencial los sábados así como los respaldos completos el primero de cada mes. Si quiere hacer esto, simplemente configure [Respaldo por deltas] → [Avanzado] → [Ajuste Avanzado de Tipo In-File Delta].

9. ¿Cómo desinstalar la aplicación?

9.1. Desinstalación en Windows

La aplicación se puede desinstalar a través de la opción “Añadir o quitar programas” o “Programas” del “Panel de control” de Windows o, también, mediante el acceso directo al desinstalador que se encuentra en Inicio → Programas → Banckup Online Backup Pro → Desinstalar.

9.2. Desinstalación en Linux

Desde la línea de comandos, Banckup Online Backup Pro se puede eliminar de la siguiente manera:

```
# sh /usr/local/obm/bin/uninstall.sh  
# rm -rf /usr/local/obm  
# rm -rf ~/.obm
```

Desinstalación finalizada.

9.3. Desinstalación en MAC OS

Desde la línea de comandos, Banckup Online Backup Pro se puede eliminar de la siguiente manera:

```
# cd $OBM_HOME/bin  
# sudo ./uninstall.sh  
# rm -rf ~/.obm
```

Reinicie su sistema para finalizar la desinstalación.

10. Glosario

10.1. Copia de seguridad

Se denomina copia de seguridad al proceso de copiar un archivo o carpeta de su ubicación actual a otra ubicación, con el objetivo de poder restaurar esos datos en caso de pérdida de información o desastre. Los datos originales quedan intactos.

10.2. Backup

Acepción anglosajona ampliamente extendida y aceptada en entornos informáticos utilizada para referirse a una copia de seguridad o al proceso de su realización.

10.3. Copia de seguridad remota

Procedimiento por el cual se realiza una copia de seguridad que se guarda en un servidor remoto al que se accede mediante el uso de una conexión a Internet de alta velocidad (ADSL o superior).

10.4. Copia de seguridad local

Procedimiento por el cual se realiza una copia de seguridad que se guarda en un dispositivo local.

10.5. Backup on-line

Acepción anglosajona ampliamente extendida y aceptada en entornos informáticos utilizada para referirse a una copia de seguridad remota.

10.6. Servidor remoto

Equipo conectado a una unidad de almacenamiento de gran capacidad que no se halla en las mismas instalaciones donde se encuentra el equipo que contiene los datos originales que se copian. Por regla general, este tipo de equipos se hallan en datacenters especializados.

10.7. Datacenter

Instalación dotada de grandes medidas de seguridad que ofrece un alojamiento con condiciones idóneas (en lo que a temperatura ambiente, alimentación y conexión a Internet se refiere) a servidores, unidades de almacenamiento y otros equipos informáticos para que las empresas tengan acceso a sus datos o a los de sus clientes.

“Centro de producción de datos” o su acrónimo “CPD”, es el equivalente castellano a este término inglés.

10.8. Unidad de almacenamiento local

Por unidad de almacenamiento local se entiende aquel dispositivo conectado directamente o por red local al ordenador que tiene el software de backup online instalado y cuya finalidad es la de almacenar de forma permanente datos digitales.

Ejemplo de unidades de almacenamiento típicas son: discos duros, discos extraíbles (“USB” o “pen”), unidades de red, etc.

10.9. Cifrado (“Encriptación”)

El cifrado es el proceso de convertir la información original (*texto plano*) en un galimatías ilegible, denominado *texto cifrado* o *criptograma*.

Es una medida de seguridad utilizada para evitar que la información que está siendo transmitida o almacenada pueda ser comprendida por un tercero, garantizando así su secreto y privacidad.

10.10. Compresión

La compresión de datos consiste en la reducción del volumen de información tratable. Con la compresión se pretende transportar la misma información, pero empleando la menor cantidad de espacio.

El método de compresión utilizado por Banckup asegura la reducción del tamaño ocupado por la información a copiar, sin pérdida de dato alguno.

10.11. Nombre de usuario

Este nombre de usuario hace referencia al e-mail introducido por el usuario al darse de alta en el servicio de backup online.

10.12. Password

Contraseña que protege la cuenta de usuario.

10.13. Frase o Clave de cifrado

Parte del mecanismo de cifrado utilizado para proteger los datos de usuario de manera que **únicamente** él puede recuperarlos de forma inteligible.

La longitud mínima de la frase de cifrado es de 20 caracteres.

La frase de cifrado debe guardarse en lugar seguro, puesto que en caso de pérdida los datos de usuario no podrán ser recuperados. Banckup **no** conoce la Frase de Cifrado de sus clientes, **sólo ellos tienen acceso a sus datos copiados**.

En caso de pérdida, el usuario puede solicitar el reseteo de dicha frase enviando un e-mail a sopORTE@banckup.com, de manera que recuperará el acceso a su cuenta pero los datos no podrán ser recuperados. El usuario deberá realizar un backup completo de todos sus backup programados.

10.14. Primera copia

Una primera copia es toda aquella información que se envía por primera vez al servidor remoto donde se almacenan sus copias de seguridad.

La realización de la primera copia es la que más tiempo conlleva, ya que toda la información de la que se quiere tener copia de seguridad es enviada al servidor remoto. Con la primera copia hecha, las sucesivas copias copian únicamente aquella información que ha variado respecto a la que ya se tenía.

10.15. Copia local

Una segunda copia es aquella información que se guarda en un dispositivo local (disco duro, unidad de red, disco USB, etc.).

Cuando se realiza una copia de seguridad contra servidor remoto y otra contra dispositivo local (segunda copia), se aumenta la protección de sus datos.

Corporate Headquarters

Banckup, c/Berlín 63 – 65, Entl. A, Barcelona, 08029 SPAIN
Tel: 93 363 72 67 Fax: 93 363 72 61



www.banckup.net

© 2010 Data Copy Systems SL.

All rights reserved.

Banckup is a registered trademark of Data Copy Systems SL.

All other trademarks, marked and not marked, are the property of their respective owners.