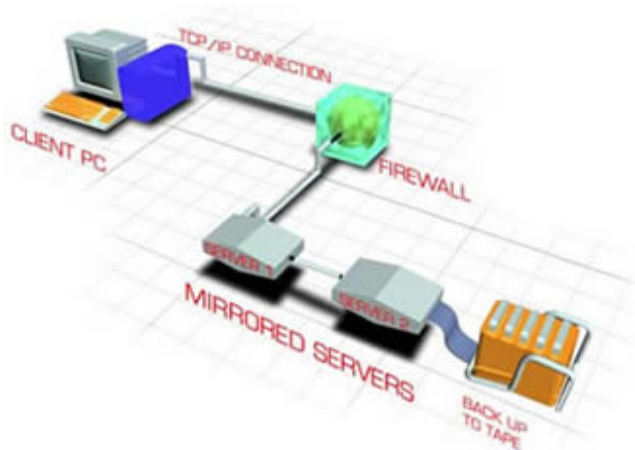




SECURE ONLINE BACKUP – HOW IT WORKS

DATBar is an advanced online data backup for Microsoft Windows ® users. The *DATBar* software runs conveniently on each user's computer to maintain a regular backup of important files to our secure backup servers (mirrored). The client and server components work together to provide a simple automated backup solution for any number of users

1. Our **backup software** is installed on the client / server workstation
2. The user creates a **schedule** for the back up
3. Data is **compressed** and **encrypted** on the client PC
4. Data is transferred via the client internet connection to our **secure data centre**
5. Data held on mirrored servers for rapid online recovery
6. Data backed up to tape providing 3rd offsite copy



N.B. The system diagram above is only a simple representation

BACKUP SOFTWARE DETAILS

SILENT MODE

A silent mode allows the program to run silently in the background without displaying any Windows or Task Bar icons. This allows the administrator to set scheduled backups to run silently at a low priority to accomplish users backups throughout the day.

EVENT MANAGER

An Event Manager is provided to alert users of any missed or failed backups. If a scheduled backup is

missed, the next time the computer is started the Event Manager will display the missed event and allow the user to immediately perform the missed event. This is useful for laptop users that may be out of the office during a regularly scheduled backup.

If a backup fails to complete successfully, the Event Manager will try the backup again when the computer is restarted or the software is executed. If a backup fails due to a network problem, the Event Manager will prompt the user to complete the backup at a later date.

EMAIL NOTIFICATION

The client software can be configured to send an e-mail to any user(s) upon any successful backup or a backup with errors or warnings. A summary of the attempt is sent in the body of the message and the complete log file may be attached as an option.

MULTIPLE BACKUP SETS

Our software features the ability to create an unlimited number of backup sets. Since backup sets can be scheduled to run independently, a user can configure multiple backup sets to run at different times. For example, a backup set containing all data files can be configured to run at the end of each week and another backup set containing a single database file can be configured to run multiple times per day. All file versions will still be immediately available for the user to restore.

SCHEDULING

Enhanced scheduling options have been added to the client software to help automate the backup process, ensuring that the user data is backed up on a regular basis without requiring user intervention. The new scheduling capabilities allow users to configure backups at any time, multiple times per day or even before Windows Shut Down. Additionally, any third party scheduling application can be used to run the backup application by scheduling simple command line calls to run an automated backup.

COMPRESSION

DATBar uses FastBIT technology that can accurately extract the changes that you've made to a file since your last backup. This efficiency is achieved by using the powerful FastBIT difference engine to identify and extract the binary-level differences on two versions of any file. The technology works on ANY type of file.

When our backup program encounters a file for the first time, it compresses the file and sends it securely to the backup server. All future changes to your files will result in only the changes within the files being sent to the server. When the changes are received by the server, they are applied to your backup files creating a complete up-to-date copy of your file system. As an optional service, your daily FastBIT Patch Backup files can be stored separately on the server allowing the flexibility of restoring any file(s) from your backup data as of any point in time. Thus allowing you to go back to restore a number of generations.

Applying FastBIT technology to the backup process will reduce your costs without sacrificing the integrity of your backups. FastBIT has been the only choice for IBM, Microsoft, Novell, and many other hardware and software companies needing to update commercially distributed software.

ENCRYPTION

All data is stored in an encrypted format and all communications between the client and server are encrypted. Users can choose between DES, Triple-DES and Blowfish encryption algorithms. The software is available with exportable levels of encryption for International customers

Encryption allows a user to specify an access code or password which is used to make computer data unreadable to anyone without the correct password. The DES algorithm is a popular algorithm that has been used by the U.S. Government as the standard encryption algorithm. Another algorithm gaining popularity is the Blowfish algorithm which allows a more powerful encryption and faster performance than DES.

DES

Adopted in 1977, DES is based on a conventional or secret key system in which the sender and the receiver use a single key to encrypt and decrypt data. The sender uses the key to convert the data to scrambled

format according to a complex mathematical algorithm, and only users with the correct key can successfully decrypt the data. Having a key length of 64 bits, 56 are used as a key, while the remaining eight are used to check for errors. The DES algorithm will encrypt data in the same amount of space used by the original data. The user selects which one of more than 72 quadrillion transformation functions are to be used by selecting a 56-bit key. The theory behind the security of DES has been that, short of trying all 72 quadrillion combinations, there is no way to "break" the algorithm.

Triple DES

To increase the security of DES, some organizations use "triple DES" - or three operations of DES with two keys - to protect data. This method, however, requires more processing power which may affect performance.

Blowfish

Blowfish was designed in 1993 as a fast, free alternative to DES. Unlike DES, however, the Blowfish algorithm has a variable key length, which can be extended from 32 bits to 448 bits. Blowfish continues to gain acceptance in the marketplace because it is faster and more secure than DES.

With *DATBar* there are several places that encryption is used to ensure that the user's data is secure.

COMMUNICATIONS

Since the information is transmitted across the Internet, the communications between the user and the server should be encrypted to prevent a malicious person from intercepting data as it is transmitted over the Internet. As part of the initial connection procedure, the *DATBar* client software negotiates a compatible set of encryption methods before sending any user information or data to the server. This ensures that all user communications during the entire backup and restore process are completely encrypted.

STORAGE ON THE SERVER

When the encrypted backup data has been successfully received by the server, it is immediately stored on the disk in the encrypted format and the filenames are further encrypted to make it more difficult for someone to identify the user data on the server. Data must be encrypted while stored on the server to prevent from an unauthorized user from accessing your data files and to protect the data in the event of the physical storage devices being obtained by an unauthorized third party.

STORAGE ON THE CLIENT

Important information such as the user's password must be stored on the client computer in order to facilitate the logon process to the *DATBar* server. This password and other important information is stored on the client system in an encrypted format that can only be read by the *DATBar* application.

USER AUTHENTICATION

User authentication is performed immediately after the encrypted connection between the client and server has been made. The client software sends the username and password to the server to be validated against the Windows NT user database. This method of user authentication provides a robust and secure method for managing users. Using the Windows NT user database provides a standard secure database of users with the ability to quickly validate users against this database.

***Online Backup* backend system**

Overview

All data is held on mirrored RAID5 storage arrays held within our data centres. A Third copy is archived using Best of Breed Backup (BOBB). BOBB is an online archiving facility which is scaleable so as to allow us to practically and economically store data for 7 years. On a daily basis a full backup of Databarracks primary and secondary storage arrays are backed up to BOBB – which itself is then mirrored in dual locations.

Currently Bo BOBB bb is mirrored within our primary data centre in Ash, but a mirror to Newbury is planned shortly.

All data that is kept on BOBB is separate from the primary 'online' storage arrays. Though BOBB is an online data archiving system, clients are not able to directly access the data archived on BOBB, but it is possible for Databarracks technicians to make data available in a clients online account within 6 hours of a request being made. It is therefore possible to allow data to be reintroduced from archive in a fraction of the time that a traditional tape archiving system would be able to.

BOBB uses proprietary incremental technology that replicates state of the art tape banks by using raid 5 serial data technology. BOBB has been developed exclusively for Databarracks by leading IT security company AL Digital. The whole system is behind a dedicated hard firewall. The firewall is constantly monitored and updated by our technicians within the bunkers to remain current.

Monitoring

The system is monitored using two software packages

- **Nagios**
- **Quest spotlight**

Nagios

Nagios is an open source host, service and network monitoring program. When problems are encountered, the daemon sends out notifications to administrative contacts via email and SMS texting. Current status information, historical logs and reports are all accessed via a web browser.

Nagios has a number of features

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, PING, etc.)
Monitoring of host resources (processor load, disk and memory usage, running processes, log files, etc.)
- Monitoring of environmental factors such as temperature
- Simple plugin design that allows users to easily develop their own host and service checks
- Ability to define network host hierarchy, allowing detection of and distinction between hosts that are down and those that are unreachable
- Contact notifications when service or host problems occur and get resolved (via email, pager, or other user-defined method)
- Optional escalation of host and service notifications to different contact groups
- Ability to define event handlers to be run during service or host events for proactive problem resolution
- Support for implementing redundant and distributed monitoring servers
- External command interface that allows on-the-fly modifications to be made to the monitoring and notification behavior through the use of event handlers, the web interface, and third-party applications
- Retention of host and service status across program restarts
- Scheduled downtime for suppressing host and service notifications during periods of planned outages
- Ability to acknowledge problems via the web interface

- Web interface for viewing current network status, notification and problem history, log file, etc.
- Simple authorization scheme that allows you restrict what users can see and do from the web interface

Quest spotlight

Spotlight on Unix graphically displays, in real time, the actual flow of data in our unix systems — including I/O subsystem, cache and kernel information — enabling us to identify congested areas and quickly respond to performance problems before they become a major concern. Spotlight also has a learning facility that automatically sets a baseline of normal activity for each system, allowing Spotlight to automatically set thresholds and send an audible or visual warning of impending problems. With these advanced notifications, we can proactively eliminate bottlenecks before they seriously impact end users.

SYSTEM REQUIREMENTS

- Windows 9x/Me/NT 4.0/2000/XP
- Pentium Class Processor
- 32 MB RAM or greater
- 5 MB Disk Space plus space required for processing
- TCP/IP Network, Dial-Up Networking (if desired)
- Modem or other networking hardware