ONLINE BACKUP MANAGER

FREQUENTLY ASKED QUESTIONS

Can you explain the concept briefly on how the software actually works?

Online Backup Suite consists of 3 main modules:
1. The client software – Online Backup Manager (OBM)
2. The server software – Offsite Backup Server (OBS)
3. The replication server – Replication Server (RS)

Online Backup Manager (OBM) is the client-side program which uploads the selected files to the Backup Server and looks after scheduled backup jobs. It also provides a user-interface for configurations of the desired backup sets. OBM supports a number of operating systems, e.g. Windows 2000, XP, 2003, Linux, Mac OS X, etc. And apart from file backups, OBM can backup a range of applications such as MS Exchange, MS SQL, Oracle, MySQL, Lotus Domino, etc.

The Offsite Backup Server (OBS) is the server-side program which can serve and store backup data from multiple OBMs⁄ backup accounts. It has a web-based Management Console for system administrators to manage the Backup Server, such as configuring system parameters, administering the backup accounts, viewing backup statistics and reports, etc. Users can also logon to this Management Console to manage their own backup account or restore their own backup data. OBS supports Windows, Linux and Mac OS platforms.

The Replication Server (RS) is another piece of server software running on a separate machine which provides close to real-time backup for multiple OBSs. Meaning, even if one of the OBSs fail, the RS still has a copy of the backup data.

What is the recommended bandwidth?

It really depends on the kind of data to be backed up, e.g. for personal file backups, the daily data transfer should be limited, while MS Exchange backup could be significant.

How can I backup a huge data set over the Internet?

If you have a lot of data (e.g. 300GB or more) to backup to the Backup Server, it would take a considerable amount of time to perform the first full backup through the Internet. You can use the *Seed Loading Utility* to backup your backup set to a local hard disk (instead of directly to the Backup Server) and then transport the backup data, using a removable hard disk, to your backup service provider. The administrator can then load all your backup files from your removable hard disk into your backup account. This could save you days (even weeks) of performing your first full backup. And since subsequent backups are incremental (only new or updated files will be uploaded to the server), the amount of data transfer should be relatively small. Please refer to OBM User Guide for details on the *Seed Loading Utility*.

What is the best way to restore a huge data set?

You can copy the data of the particular backup set on OBS to a removable media, e.g. external hard disk, and ship it to your client. Your client can then use the Decrypt Files Tool in OBM to restore the backup data on removable media to its original format.

Can I change my encrypting key?

Once set for a Backup Set, the encrypting key cannot be changed. This is necessary for the integrity of the Backup Set, making sure that backup data is only encrypted by one key. Otherwise, you will have problems remembering two encrypting keys when you want to restore your files in the future. You need to recreate your Backup Set if you really want to change your encrypting key.

What kind of encryption is employed by OBM?

There are two encryptions being performed by OBM:

1. Encryption of backup data - This is being done by 128-bit symmetric key encryption (AES, TripleDES, TwoFish). 256-bit is not available because it requires too much CPU and it is not really required (128-bit is what is being used by most banks currently).

2. Encryption of backup traffic - This is being done by 1024-bit RSA public key encryption. The strength of the encryption depends on the key size you use when you generate your CSR before submitting to your CA (1024-bit is what is being used by most CAs).

Can I backup an entire Operating System?

Currently, it is not possible to do hard disk image backup with OBM. However, you can still backup and restore the operating system by following the instructions below.

To backup all files including the operating system, please do this:

1. Add all files to your backup source.
2. Add a SystemState backup type to your backup account (Windows only).

To restore all files including the operating system, please do this:

1. Re-install the operating system and applications.
2. Restore the SystemState backup to your machine (Windows only).
3. Restore all files to your machine.

What are the upsides and downsides of backing up multiple computers using a single backup account?

Upsides:

· You require less backup accounts.
· You can use one pair of username and password to configure the backup setting of all backup settings.

Downsides:

· You must use different backup sets for different computers.
· Whenever a new backup set is created under the backup account, you need to go back to all computers using the same backup account to uncheck the "Run scheduled backup on this computer" option for the new backup set (as backup setting is saved on server and new backup set is default to run on all computers, i.e. with the option checked).
· Improper configuration could easily cause problems, which are difficult to debug.

Does OBM upgrade the installation of Java on a client machine, or does it install a separate copy for its own use?

OBM uses its own copy of Java and leaves the system Java VM intact.

How does the "Remove retention files for overlap policy" under Advanced Retention Policy work?

In general, daily snapshots followed by a weekly snapshot or a monthly snapshot, etc. will be removed; weekly snapshots followed by a monthly snapshot or a quarterly snapshot, etc. will be removed; and so on.

This is illustrated by the following example: Assume today is 17Jan06, and the Advanced Retention Policy is as follows: - Daily: retain for 7 days - Weekly: retain for 4 weeks (the job will be performed on Saturday) - Monthly: retain for 3 months (the job will be performed on 1st of each month).

If "Remove overlap policy" *IS NOT* enabled then a total of 14 snapshots (7+4+3) will be kept on the server accordingly, i.e.: (daily) 10Jan06, 11Jan06, 12Jan06, 13Jan06, 14Jan06, 15Jan06, 16Jan06 (weekly) 24Dec05, 31Dec05, 7Jan06, 14Jan06 (monthly) 1Nov05, 1Dec05, 1Jan06.

If "Remove overlap policy" *IS* enabled then only the following snapshots are kept: 1Nov05, 1Dec05, 1Jan06, 14Jan06 15Jan06, 16Jan06. Specifically, the weekly policy overrides the daily policy so 10Jan06, 11Jan06, 12Jan06 and 13Jan06 will be removed. The monthly policy overrides the weekly policy, and 24Dec05, 31Dec05 and 7Jan06 will be removed as well.

What is incremental backup and how does In-File Delta work?

In an incremental backup, only modified files will be uploaded to the Backup Server. On the other hand, In-File Delta is applicable to the physical files to be uploaded to the Backup Server, does not matter whether it is a MS SQL database file, MS Exchange transaction log file or any normal file in a FileBackupSet.

Specifically, only the changed blocks in comparison to the original file on the Backup Server (delta file) will be uploaded. For each modified file, OBM would determine whether the entire file or only delta file should be uploaded. If the entire file is to be uploaded, the old version of the file will be moved to the Retention area. Else if only the delta file is to be uploaded, the previous delta files will be moved to the Retention area and the Data area should contain the original full backup file, checksum file and the latest delta file of this file.

Does OBM have to stop an application when doing online backups?

OBM can backup application data while other applications are still running. Particularly, we have special agents for MS Exchange Server, MS SQL Server, Oracle, Lotus Notes and MySQL, which allows these applications to be backed up while they are online. With the introduction of the Volume Shadow Copy feature started from OBM v5.0, we are now able to backup other types of applications while they are online.

What are the Off-line Backup, Logout Backup Reminder and Local Backup features?

Off-line Backup is basically designed for notebook users who are off-line most of the time and cannot rely on the backup schedule to backup regularly. The backup interval allows notebook users to specify the interval that they would like their data to backup. If this interval has elapsed, backup will run automatically once this machine is online.

Logout Backup Reminder asks user if they would like to backup if they logout of, or shutdown, their computer.

Local Backup allows an extra copy of the backup file to be kept on a local hard disk when running the backup.

Does OBM work with dial-up connections?

It makes no difference to OBM if the connection is always on or dial-up. If you want Windows to connect to the ISP automatically when a backup starts, navigate in Windows to the following:

Control Panel > Internet Options > Connections > Always dial my default connection

What do I have to do in order to backup open files?

Volume Shadow Copy, which allows backup of open file, comes with Windows XP and 2003 by default. For older platforms, e.g. Windows 9x/ME/NT/2000 or NetWare, we would recommend adding a third party open file manager option*. For instance, St. Bernard's Open File Manager (www.stbernard.com) which might cost around US$100 for each workstation and US$300 for each server if open file backup is required.

* Open file option is not required on Linux/Unix/Mac OS X because no files are held exclusively open by applications.

How does Volume Shadow Copy work?

Please refer to the following search criteria:

1. **http://technet2.microsoft.com** (clickable in Adobe Reader or Acrobat).
2. In the Search field, enter "*Volume Shadow Copy*" and read the corresponding article.

Is there a way to backup Oracle 7.3.4 on NetWare?

To backup Oracle 7.3.4 on NetWare 5.1, it is not possible to use the Oracle agent.

You will need instead to do the following:
1. Backup all Oracle 7.3.4 datafiles, control files, and pfile.
2. Use “exp” (export utility) to dump Oracle database to a dump file (make this a pre-backup command).
3. Use OBM to backup this file.

When you need to restore the database, just restore all datafiles, control files and pfile to its original location and use “imp” (import utility) to put the data back into Oracle database.

How is the data privacy being maintained on OBS?

All data is encrypted with the user’s defined encrypting key before they are sent to the online Backup Server. The encrypting key is not stored on OBS. Without the encrypting key, the backup files are useless to anyone. The backup user is the only person who can decrypt the backup files to reveal the original content.

What is the recommended hardware and Operating System (Windows or Linux) for OBS?

As a rule of thumb, an active backup connection takes roughly 256KB of memory. Thus, a 512MB heap size can easily support over 2000 active backup connections. The required storage space depends on the expected amount of backup data from your users, and it is possible to make use of an external storage server.

Most processing is done on the client side, thus CPU utilization on the OBS machine shouldn’t be intensive. For your reference, in most circumstances, a P4 2.8GHz CPU with 1GB of RAM and lots of disk space (2-4TB of disk space) can support up to 500 users. OBS runs equally well on Windows and Linux platforms. You may want to go for a platform that your system administrators are comfortable with. From the operating system point of view, Linux might be more stable and require less maintenance.

Is there an example of how the Retention area works?

Suppose you have 10GB of initial data which grows by 200MB (0.2GB) per day, and on each day 100MB (0.1GB) of the data is modified or deleted from the client machine. Assume the default retention policy setting is used, i.e. 7 days. Then:

Day 1: Data = 10.2G; Retention = 0.1G; Total quota used = 10.3G;
Day 2: Data = 10.4G; Retention = 0.2G; Total quota used = 10.6G;
....
Day 8: Data = 11.6G; Retention = 0.7G; Total quota used = 12.3G; (the 0.1G from Day 1 is removed from Retention)
Day 9: Data = 11.8G; Retention = 0.7G; Total quota used = 12.5G; (the 0.1G from Day 2 is removed from Retention)

Which means, if data is not being modified or deleted frequently, then the size of the Retention area should be minimal.