Table of Content

1 FAQ

1.1 Can you briefly explain the idea of how the Ahsay Online Backup Software works?

Answer) Ahsay Backup Software consists of four major components, in which two of them are server-side applications (AhsayOBS and AhsayRPS) and the other two are client-side applications (AhsayOBM and AhsayACB).

Ahsay™ Offsite Backup Server (AhsayOBS) is the core server application of Ahsay Backup Software. Offering centralized backup services to diverse AhsayOBM and AhsayACB users, which allows system administrators to manage individual users and their account configurations, as well as monitor the entire system's performance easily.

Ahsay™ Replication Server (AhsayRPS) is a server application for storing data replicated from one or multiple AhsayOBS, aimed to provide an additional level of protection to the backed up data.

Ahsay™ Online Backup Manager (AhsayOBM) is a comprehensive client-side application available with various database backup modules to backup files and databases from client-side computers to AhsayOBS, which is most suitable to backup servers.

Ahsay™ A-Click Backup (AhsayACB) is a light version of AhsayOBM with all major features retained while having an easy-to-use interface, which is most suitable to backup desktops and laptops.

The relationships of the Ahsay Online Backup Suite are depicted in the diagram below:
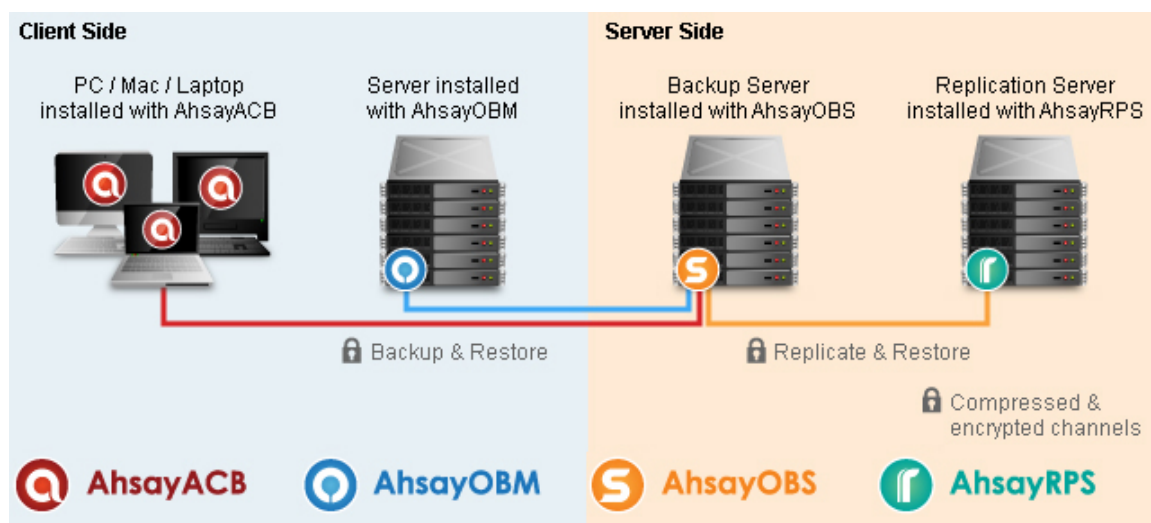
1.2 Are there any command line tools for AhsayOBM / AhsayACB?

Answer) Yes, there are script files available in the ${Install-Home}\bin folder:

Windows

- Decrypt.bat: Decrypts the specified backup files
- RegisterVSS.bat: Re-registers Microsoft's Volume Shadow Copy service DLLs
- Restore.bat: Restores the specified snapshot of the backup set to the specified location
- RunBackupSet.bat: Runs the specified backup set
- RunMailBackup.bat: Runs the specified MS Exchange mail level backup set
- RunOBM.bat: Launches the Ahsay Online Backup Manager user interface
- Run-Scheduler.bat: Starts the Ahsay Online Backup Scheduler service
- SeedLoad.bat: Runs seed load for the specified backup set to the specified location

Linux

- BackupManager.sh: Launches the Ahsay Online Backup Manager user interface
- Configurator.sh: Configures client parameters such as Backup Server address, username/password, encrypting key, etc.
- Decrypt.sh: Decrypts the specified backup files
- Restore.sh: Restores the specified snapshot of the backup set to the specified location
- RunBackupSet.sh: Runs the specified backup set
- Scheduler.sh: Starts the Ahsay Online Backup Scheduler service
- SeedLoad.sh: Runs seed load for the specified backup set to the specified location
- StopScheduler.sh: Stops the Ahsay Online Backup Scheduler service

*Detailed instruction on how to use each script can be found within the respective script file.

1.3   How does AhsayOBM / AhsayACB detect change in files, does it use the Archive bit?

Answer) AhsayOBM / AhsayACB compares timestamps of files on the server with the corresponding copies on client machine. Archive bit is not used as it does not detect relocated files. Therefore tape backup would not affect Ahsay's backup application.

1.4   Does AhsayOBM / AhsayACB copy the same set of files regularly?

Answer) After the initial upload, subsequent backup jobs will only transfer the modified or new data to the Backup server.

1.5   Does In-file Delta backup require a temporary working directory?

Answer) Yes, AhsayOBM / AhsayACB requires a temporary storage for the delta file before it is sent to the server.

For a 10 GB file that has already been uploaded to the AhsayOBS server, if there is an updated of 10 MB to this file, the temporary storage must have at least 10 MB of free space.

For five 10 GB files in the same situation. The require space for temporary storage will be need 10 MB (instead of 5 times 10 MB), because each delta file will be automatically deleted right after it has been backed up.

1.6   What is the average compression ratio?

Answer) All backup files are compressed and encrypted before uploading to the Backup Server, the average compression ratio for text-based file is around 4:1.

However, no further compression can be made on files that are already in compressed format (e.g. JPG, ZIP). In general, you can assume a 2:1 compression ratio when you are backing up a file set with variety types.

1.7   What kind of encryption used by AhsayOBM / AhsayACB?

Answer) There are two encryptions being performed by AhsayOBM:

- Encryption of backup data - This is being done by 256 or 128 bit symmetric key encryption (AES, TripleDES, TwoFish).
- 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.

1.8   Does the AhsayOBM / AhsayACB upgrade the installation of Java on a client machine?

Answer) AhsayOBM / AhsayACB uses its own copy of Java and leaves the system Java VM intact.

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

Answer) 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 File BackupSet. Specifically, only the changed blocks in comparison to the original file on the Backup Server (delta file) will be uploaded.

For each modified file, AhsayOBM / AhsayACB 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.

1.10   How does the 'Auto' block size work under In-file Delta settings?

Answer) If the block size is set to 'Auto', the effective block size will be chosen from the following table based on the file size of the updated file:

File Size	Delta Block Size
0 - 500 MB	4k
500 MB - 2 GB	8k
2 GB - 8 GB	16k
8 GB - 15 GB	32k
> 15 GB	64k

1.11   What are Off-line backup, Logout backup reminder and Local backup features?

Answer) To further explain these features:

- Off-line Backup is basically designed for notebook users who are off-line most of the time, and cannot rely on 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 the computer or shutdown their computer.
- Local Backup allows an extra copy of backup file to be kept on local hard disk when backup is running.

1.12 How do I remove AhsayOBM completely from my Windows machine?

Answer) If you want to completely remove AhsayOBM from Windows, after uninstallation of the application is completed, please:

- Remove the AhsayOBM / AhsayACB installation directory
- Remove the user profile folder (.obm)

1.13 Does AhsayOBM / AhsayACB work with dial-up connections?

Answer) It makes no difference to AhsayOBM / AhsayACB if the connection is always on or dial-up.

1.14 Does AhsayOBM have to stop the application when a backup is performed?

Answer) AhsayOBM can backup application data while the application is still running. Particularly, we have special agents for MS Exchange Server, MS SQL Server, Oracle, Lotus Domino and MySQL, which allows these applications to be backed up while they are online.

1.15 How do I install AhsayOBM on a FreeBSD machine?

Instructions:
1. Download the latest version of AhsayOBM (obm-nix.tar.gz)
2. Download and install the Diablo JRE 1.5.0-7 to the following directory: /usr/local/diablo-jre-1.5.0.07.01_3

   Notes:
   Depending on the BSD release, you can download the corresponding Diablo JRE and dependant packages from the following locations:

   FreeBSD Foundation Java Downloads
   FreeBSD Project

3. Unpack the obm-nix.tar.gz package to the following directory: /usr/local/obm

   Example:
   >mkdir /usr/local/obm
   >cd /usr/local/obm
   >tar -zxvf obm-nix.tar.gz

4. Remove the bundled Java version:

Example:
>rm -rf /usr/local/obm/jvm

5. Create a symbolic link to the Diablo JRE that was previously installed in Step 2:

    Example:
    >ln -s /usr/local/diablo-jre-1.5.0.07.01_3 /usr/local/obm/jvm

6. Install the AhsayOBM software with the following command:

    Example:
    >./bin/install.sh > install.log

    Notes:
    The installation log file can be found in the generated install.log

7. Install the backup scheduler and auto upgrade services with the following instructions:

    i.   Add two entries to system file /etc/rc.conf for auto starting backup scheduler and
         autoupgrade agent:

         obmaua_enable="YES"
         obmscheduler_enable="YES"

    ii. Finally, restart the computer or run the following scripts to complete the installation

         /usr/local/etc/rc.d/obmscheduler start &
         /usr/local/etc/rc.d/obmaua start &

1.16 How do I install AhsayOBM on a Sun Solaris Unix machine?

Assumptions:
You have logged into the Unix machine as root

Instructions:
Please refer to the following instructions:

1. Download the latest version of AhsayOBM (obm-nix.tar.gz)

2. Download and install J2SE Java Runtime Environment (JRE) 1.4.x or later to the following
    directory: /usr/java

3. Unpack the obm-nix.tar.gz package to the following directory: /usr/local/obm

    Example:
    >mkdir /usr/local/obm
    >cd /usr/local/obm
    >tar -zxvf obm-nix.tar.gz

4. Remove the bundled Java virtual machine:

    Example:
    >rm -rf /usr/local/obm/jvm

5. Create a symbolic link to the J2SE Java Runtime Environment (JRE) that was previously installed
    in Step 2:

    Example:
    >ln -s /usr/java /usr/local/obm/jvm

6. Install the AhsayOBM software with the following command:

   Example:
   >./bin/install.sh > install.log

   Notes:
   The installation log file can be found in the generated install.log

1.17 How do I install AhsayOBM on a IBM AIX, SCO, or HP Unix machine?

Assumptions:
You have logged into the Unix machine as root

Instructions:
Please refer to the following instructions:

1. Download the latest version of AhsayOBM (obm-nix.tar.gz)

2. Unpack the obm-nix.tar.gz package to the following directory: /usr/local/obm

   Example:
   >mkdir /usr/local/obm
   >cd /usr/local/obm
   >tar -zxvf obm-nix.tar.gz

3. Remove the bundled Java virtual machine:

   Example:
   >rm -rf /usr/local/obm/jvm

4. Create a symbolic link jvm to the Unix Java VM from /usr/local/obm:

   Example:
   >ln -s %JAVA_HOME% jvm

   Notes:
   %JAVA_HOME% is the Java VM home on the Unix Machine in concern (e.g. /opt/java1.4)

5. Create a symbolic link jvm to the Unix Java VM from /usr/local/obm/aua:

   Example:
   >ln -s %JAVA_HOME% jvm

6. Change the owner and group of SchedulerOBM, ObmJW, and AuaObmJW to the same owner and group as java:

   Example:
   >cd %JAVA_HOME%/bin

   >cp java SchedulerOBM
   >cp java ObmJW
   >cp java AuaObmJW
   >chmod 755 SchedulerOBM
   >chmod 755 ObmJW
   >chmod 755 AuaObmJW

7. Run the Configurator.sh script within the AhsayOBM installation home to configure the connection to the AhsayOBS server:

Example:
>cd /usr/local/obm/bin/
>./Configurator.sh

8. Start the AhsayOBM Scheduler by running the Scheduler.sh script within the AhsayOBM installation home:

Example:
>cd /usr/local/obm/bin/
>./Scheduler.sh

9. Finally, start the AhsayAUA Service by running the startup.sh script within the AhsayOBM installation home:

Example:
>cd /usr/local/obm/aua/bin
>./startup.sh

1.18 How do I uninstall AhsayOBM / AhsayACB completely from my Windows machine?

If you want to completely remove AhsayOBM / AhsayACB from a Windows machine, please follow the instructions below:

1. From the Windows Start menu, select Programs, and AhsayOBM / AhsayACB

2. Select Uninstall from the list and press the Yes button

Example of AhsayOBM un-installation on Windows XP Professional:
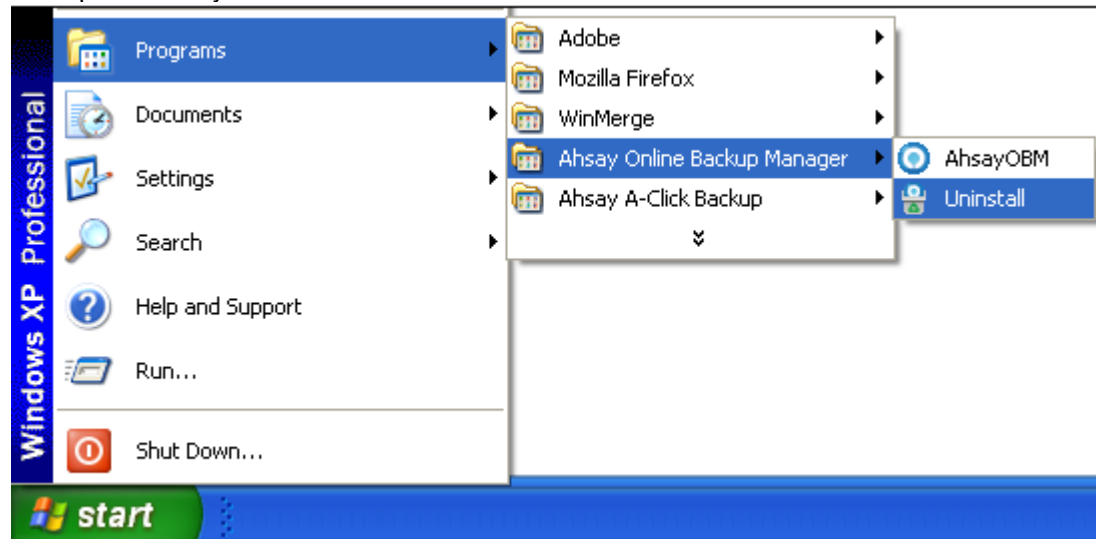
3. When prompted to remove User Setting, press Yes

Example of AhsayOBM uninstallation:
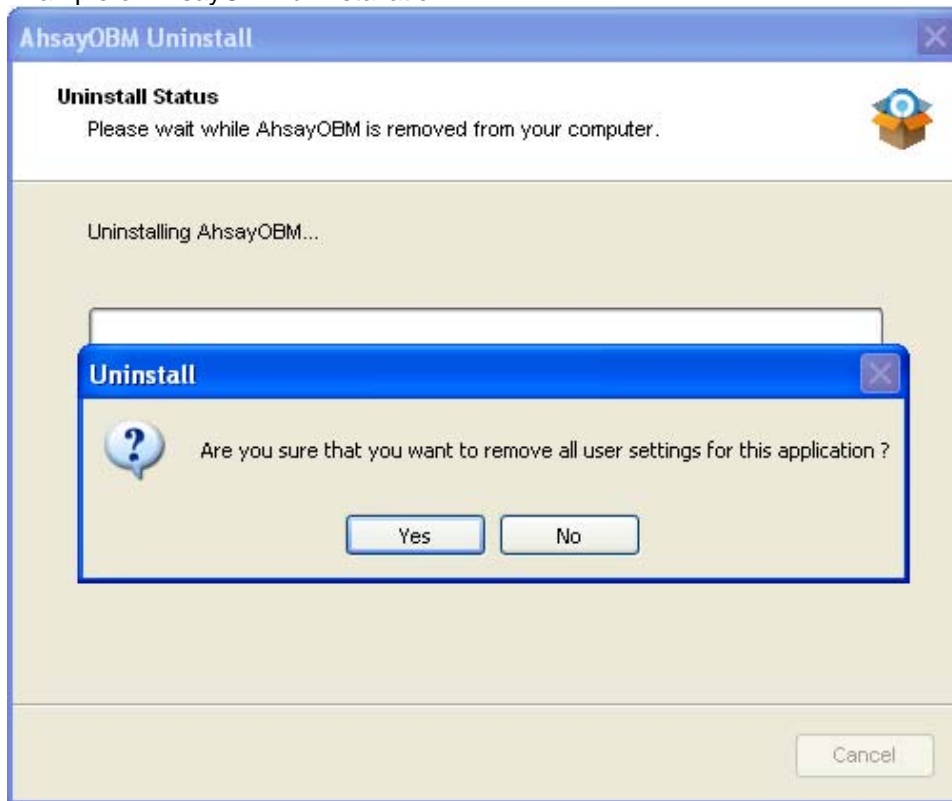
4. Remove the AhsayOBM / AhsayACB installation directory ${OBM-Install-Home} / ${ACB-Install-Home}

If you want to completely remove AhsayOBM / AhsayACB from a Mac OS X machine, please follow the instructions below:

1. Remove all program files by running the following command:

    Example for AhsayOBM uninstallation:
    >cd /Applications/Ahsay\ Online\ Backup\ Manager/bin
    >sudo sh ./uninstall.sh

    Example for AhsayACB uninstallation:
    >cd /Applications/Ahsay\ A-Click\ Backup/bin
    >sudo sh ./uninstall.sh

2. Remove all user setting by running the following command:

    Example for AhsayOBM uninstallation:
    >sudo rm –rf ~/.obm

    Example for AhsayACB uninstallation:
    >sudo rm –rf ~/.acb

If you want to completely remove AhsayOBM from a Linux machine, please follow the instructions below:

1. Remove all program files by running the following command:

    Example:
    >cd /usr/local/obm/bin
    >sudo sh ./uninstall.sh

2. Remove all installation files by running the following command:

    Example:
    >sudo rm –rf /usr/local/obm

3. Remove all user setting by running the following command:

    Example:
    >sudo rm –rf /root/.obm

1.19 Does user password change equals to encrypting key change?

In most cases, a change in the password will not leads to a change of encrypting key.

This is because encrypting key is configured when a backup set is created. Thus, even if the password is changed afterward, the encrypting key will remain the same.

However, there can be exceptional case where the client have modified his/her password, and then login to AhsayOBM / AhsayACB (with the same backup account) on a different machine, or if the .obm folder has been removed from the corresponding machine (the .obm folder is where the user profiles, settings ... etc. are stored). As the user logs in, the client software will prompt for the encryption key setting for the backup sets that existed with the account:

Example with Default setting:
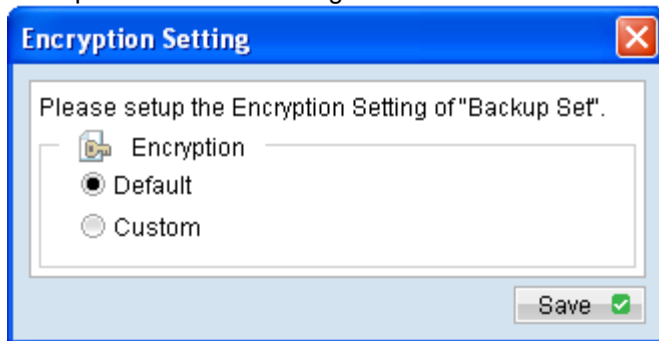
At this time, if the user have modified the password, he/she should select the "Custom" option, and enter the previous password as the encrypting key:

Example with Custom setting:
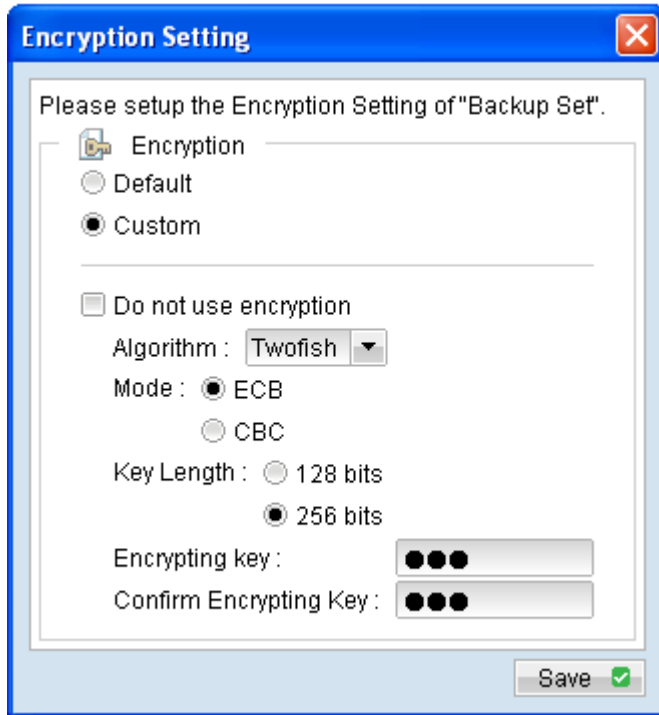
In the case where the user selects the "Default" option (which is to use the updated password as encrypting key), data of this particular backup set will then contain two encrypting key. To recover from such case, please refer to Step 4 - 6 in the "Also See" section.

1.20 Lost of user password or encrypting key?

Lost of User Password:
In the case where your user password is lost, you can retrieve it by requesting the "forgotten password" email from the web console. The password provided in the email will actually be a hashed version of the user password, the actual password is never stored on the AhsayOBS server for security reason.

The hashed password provided in the email can then be used to login to the AhsayOBM / AhsayACB client software, however, the hashed password cannot be used to decrypt data. Even if the encrypting key configured to be the same as the user password.

In the case where the backup set encryption setting is set to default (to use password as the encrypting key), you will need the actual password to decrypt any data backed up. This includes data previously backed up and also data that is backed up in the future for existing backup sets.

Lost of Encrypting Key:
In the case where your encrypting key is lost, there will be no way to restore data from the corresponding backup set. You must create a new backup set and then backup the data again in order have a restorable copy of the data. Since the encrypting key is never sent to the AhsayOBS server, thus, the encrypting key is not retrievable if lost.

If the encrypting key is lost, then the following steps must be performed to ensure that data backed up in the future can be restore and decrypt:

1. Delete all backup sets where the encryption key is lost
2. Create new backup sets for the affected data
3. Backup the data immediately

We would like to stress that it is **very important** to keep a record of your user password and encrypting key.

1.21 When is a file moved from the Data area to Retention?

Answer) A file is moved from Data area to Retention area of AhsayOBS when it is modified or removed on the source machine.

1.22 How long will the file(s) be kept in the Retention?

Answer) Retention policies define what files in Retention area should be kept, retained files no longer covered by the Retention policy will be deleted from Retention area and the corresponding file versions will no longer be recoverable. In other words, a 7 day, 5 week, 13 month, 5 year policy does not mean creating 30 copies of the backup data.

1.23 Can you tell us more on how Retention Policy works?

Answer) Yes, let's look at some examples here:

Assuming the following retention policy is set: 7 day, 5 week, 13 month, 5 year retention policy

    i.   A file that has not been changed for 5 years will remain in Data area and no copies will be made
    ii.   A file modified once in the 2nd year will have the current version stored in Data area and the previous version in Retention area after 5 years
    iii.   A file created and removed within a year, for example, it never exists in Data area during any of the year end jobs, thus is not covered by the 5 year policy, will be removed within 13 months, depending on how file is being covered by the monthly policy
    iv.   When performing a file backup, only new or modified files will be backed up. In other words, even if you set a full file backup to be run on a particular day, it will only pickup files that have deltas and are modified since the last backup.

1.24 What about the "Remove retention files for overlap policy" option?

Answer) The "Remove retention files for overlap policy" option could be used if the user wants to further reduce the amount of required storage while complying with his backup policies. Let's look at an example here:

For instance, a company requires backups of its sales database at the end of each month, and once they got this month-end backup, those daily backups for that month would become redundant. i.e. Once they got the 30th Jun backup, all 29th Jun, 27th Jun, ... 1st Jun backups are not longer needed. In this case, they could set a Daily retention policy of 31 days, plus a Monthly policy for the end of each month, and then enable the "Remove retention files for overlap policy" option. This would effectively remove the files retained by daily backups proceeding the end of month backup.

1.25 Are there any recommendation on how the retention policy should be set?

Answer) We would suggest that, the retention policy set should be longer that the typical frequency of use for the files in the backup source. In other words, if a particular set of file is only used once quarterly, then the backup data should be retained for more than a quarter.

1.26 How do I setup AhsayOBM to backup Microsoft Exchange Server 2007?

Backing up information store (server level):

1. Download and install the AhsayOBM application on the Microsoft Exchange 2007 server:

    i.   (v5.2) You need to download the 64bit version of AhsayOBM (obm-win-jvm16x64.exe)
    ii. (v5.5) Download the AhsayOBM (obm-win.exe)

         Notes:
         For AhsayOBM version after 5.5.1.0, the 32bit and 64bit installer has been bundled together.

2. The information store backup can be performed with the backup procedure provided in our AhsayOBM User's Guide. For more details, please refer to Chapter 12 for full instructions

Backing up individual emails (mail-level):

1. Download and install the AhsayOBM application on the Microsoft Exchange 2007 server:

    i.   (v5.2) You need to download the 64bit version of AhsayOBM application (obm-win-jvm16x64.exe)
    ii. (v5.5) Download the AhsayOBM application (obm-win.exe)

         Notes:
         For AhsayOBM version after 5.5.1.0, the 32bit and 64bit installer has been bundled together.

2. Download and install Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 (ExchangeMAPICdo.exe)

3. Download a 32-bit Java Runtime Environment:

    i.   (v5.2) obm52-x64-i386ext.zip
    ii. (v5.5.1.0) obm55-x64-i386ext.zip

    Notes:
    The 32-bit Java Runtime Environment is already bundled with AhsayOBM version 5.5.3.0 or above.

4. Expand the zip file into C:\Program Files\AhsayOBM

5. Start the AhsayOBM application in 32bit mode:

    i.   (v5.2) Run C:\Program Files\AhsayOBM\bin\RunOBM32.bat
    ii. (v5.5) Run C:\Program Files\AhsayOBM\bin\RunOBC32.bat

6. Create a new backup set by selecting [Backup Setting] -> [Add] -> [MS Exchange Mail Level Backup] from the lower left menu of the AhsayOBM user interface

7. Follow the instructions of the backup set wizard to complete the configuration of the new mail level backup set

8. Perform the mail-level backup immediately by selecting [Backup], or let the backup job to be performed at its scheduled time.

Notes:
Since Microsoft Exchange Messaging Application Program Interface (MAPI) is only available in 32bit, and that it is not possible to run both 32bit and 64bit modules within a single process. Thus, you need to download the 32-bit Java Runtime Environment.

Further information:

Please note that, for the backup of the information store (server level), you need to utilize the 64bit mode of AhsayOBM. To run AhsayOBM in 64bit mode, please start AhsayOBM by doubling clicking on the system tray icon.

On the other hand, for the backup of the individual emails (mail-level), you need to utilize the 32bit mode of AhsayOBM. To run AhsayOBM in 32bit mode, please:

i.   (v5.2) Run C:\Program Files\AhsayOBM\bin\RunOBM32.bat
ii.   (v5.5) Run C:\Program Files\AhsayOBM\bin\RunOBC32.bat

For backup job that is performed by the scheduler services, the RunMailBackup.bat script that is located at C:\Program Files\AhsayOBM\bin\ will automatically select the correct Java Virtual Machine to be ran.

1.27 How do I perform restore for my Microsoft Exchange Server 2007?

Restoring information store (server level):

1. Create a directory for the restore of the Microsoft Exchange 2007 database files

2. Restore the database files with AhsayOBM (to the directory created in Step1)

3. Download the Exchange Recovery Utility (ExRestoreX64.zip)

4. Expand the zip file to get the Exchange Recovery Utility executable file

    Notes:
    The Exchange Recovery Utility is already bundled with AhsayOBM version after 5.2.5.0

5. Dismount the database to be restored, using the Exchange Management Console -> [Server Configuration] -> [Mailbox] -> Right-click on the database to be recovered, and select [Dismount Database]

    Example:
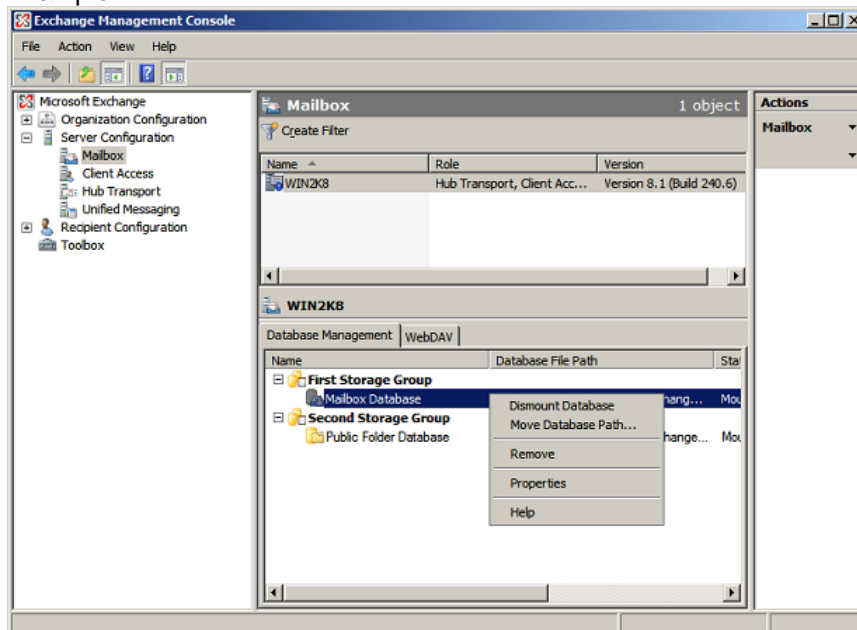
6. Run the Exchange Recovery Utility executable file (ExRestoreX64.exe) via the command prompt (Run as administrator), and then follow the usage instructions for the recovery of the database

7. Mount the database(s) using Exchange Management Console -> [Server Configuration] -> [Mailbox] -> Right-click on the database(s) that you have just dismounted, and select [Mount Database] Example: Exchange Management Console -> [Server Configuration] -> [Mailbox] -> [Mount Database]
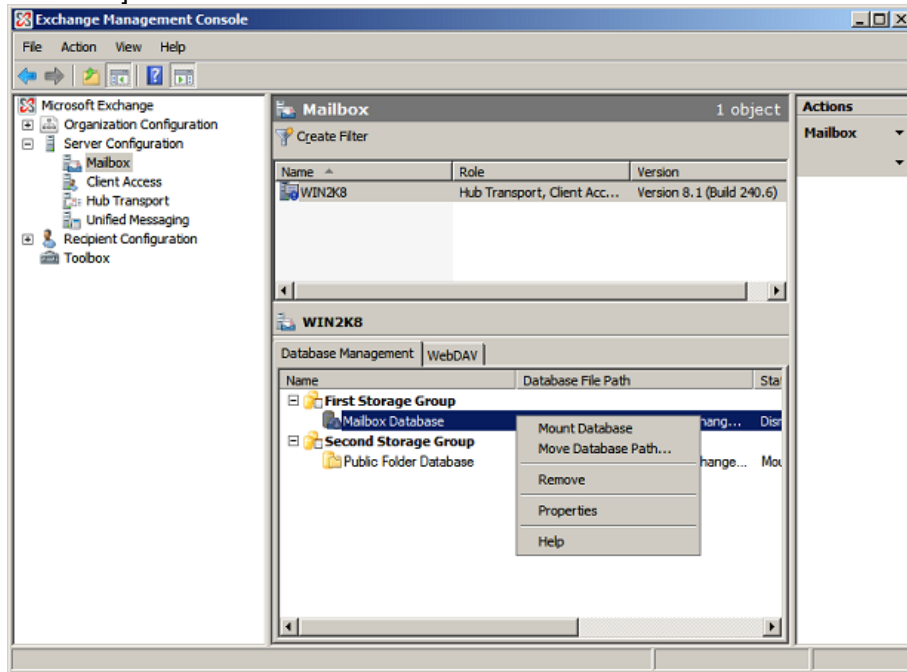
Restoring individual emails (mail-level):

To restore individual emails to the corresponding Microsoft Exchange 2007 server, you need to utilize the 32bit mode of AhsayOBM. To run AhsayOBM in 32bit mode, please:

i. (v5.2) Run C:\Program Files\AhsayOBM\bin\RunOBM32.bat
ii. (v5.5) Run C:\Program Files\AhsayOBM\bin\RunOBC32.bat

The individual emails can be restored with the restore procedure provided in our AhsayOBM User's Guide. For more details, please refer to Chapter 14 for full instructions.

1.28 MS Exchange server backup vs. mail level backup?

MS Exchange server backup module:
By performing backup on a MS Exchange server with AhsayOBM's Exchange server backup module, it allows you to recover the database in the event of a disaster, as well as allowing you to restore all mailboxes (all at once).

MS Exchange mail level backup module:
On the other hand, by performing backup on a MS Exchange server with AhsayOBM's Exchange mail level backup module, it allows you to restore individual mailboxes, folder, or messages. This is the only way to perform individual mailbox restores, as an information store restore will restore all mailboxes as part of the database restore. However, please note that by only performing backup to the Exchange server with the mail level module, it would not be possible to recover the full database in the case of disaster. Mail level backup is only supplementary to the server level backup, but it could never replace it.

In other words, an Exchange server backup is required for full server protection.

1.29 How do I backup SharePoint 2003 with AhsayOBM?

To backup your Windows SharePoint Services 2003 with AhsayOBM, please follow the instructions below:

1. Install the AhsayOBM application onto the machine running Windows SharePoint Services 2003

2. Download the wss2k3-backup.bat file by Clicking Here

3. Extract the wss2k3-backup.zip file within the ${OBM-Install-Home}\bin directory

4. Open the wss2k3-backup.bat file with a text editor, modify the following parameters according to the SharePoint server's configuration:

   - SET STSADM
   - SET URL
   - SET BACKUP

   Notes:
   Details of the three parameters can be found within the batch file itself.

5. Save the changes in wss2k3-backup.bat

6. Create the directory C:\backups

7. Open the AhsayOBM console, create a file backup set for the SharePoint backup under the AhsayOBM console

8. Select the directory C:\backups as Backup Source of the SharePoint backup set

9. Accept the default encryption settings by pressing the [OK] button if no change is necessary

10. Select the SharePoint backup set in the [Backup Setting] menu, select the [Command Line Tool]

11. Press the [Add] button under the Pre-Backup section on the right panel, enter the following entries in the corresponding text fields:

    Example:
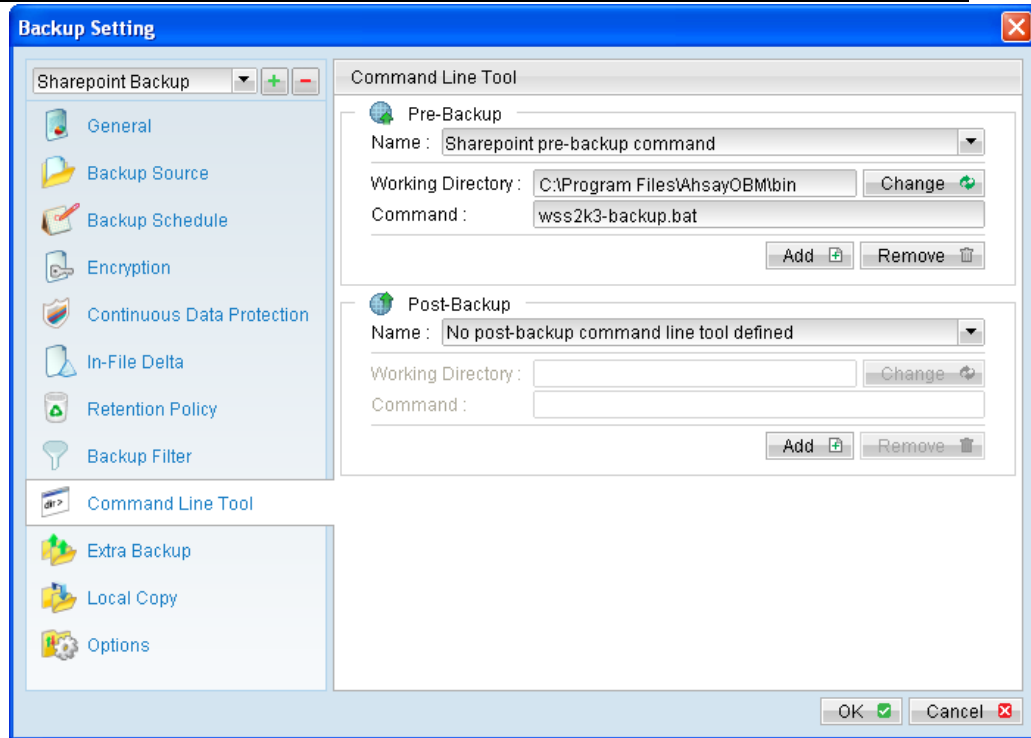
12. Press the [OK] button to save this setting

The Windows SharePoint Services 2003 server can now be backed up by pressing the [Backup] button on the AhsayOBM console.

1.30 How do I restore SharePoint 2003 with AhsayOBM?

To restore your Windows SharePoint Services 2003 with AhsayOBM, please follow the instructions below:

1. Open the AhsayOBM console

2. Open the Restore page by selecting the [Restore] button on the AhsayOBM console

3. Select the SharePoint backup set from the backup set list, and browse to the backup.dat file

   Example with the backup.dat file located in C:\backups\backup.dat:
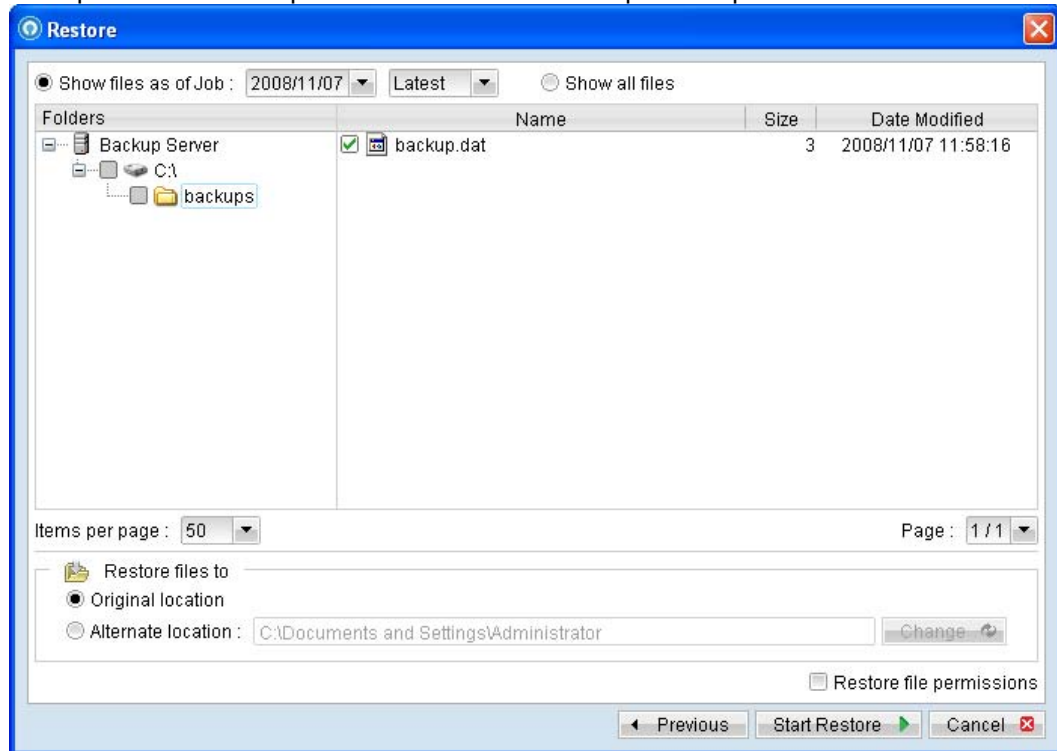
4. Select the checkbox next to the backup.dat node and press [Start Restore]

5. Open the command prompt and navigate to the directory that stsadm.exe resides in:

   Example:
   >cd "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\BIN"

6. To begin the Windows SharePoint Services restoration, enter the command:

   Example:
   >"stsadm.exe -o restore -url http://server_name/site -filename backup.dat" to begin the restoration

1.31 How do I backup Sharepoint 2007 with AhsayOBM?

To backup your Windows Sharepoint Services 2007 with AhsayOBM, please follow the instructions below:

1. Install the AhsayOBM application onto the machine running Windows Sharepoint Services 2007

2. Download the sps2k7-backup.vbs file by Clicking Here

3. Place the sps2k7-backup.vbs file within the ${OBM-Install-Home}\bin directory

4. Open the sps2k7-backup.vbs file with a text editor text editor and you should see entries as shown below:

sps2k7-backup.vbs:

```
" This script works only in Windows OS


" The directory which stores the sharepoint backup
Const BackupDirectory = "D:\BackupDir"


" This is the default path of stsadm.exe. If you have different settings, please find out the absolute path of the execute file.
Const StsadmExecPath = "C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\BIN\stsadm.exe"
```

5. Verify if the BackupDirectory and StsadmExecPath variable within the sps2k7-backup.vbs file require modification

6. Modify the backup schedule:

sps2k7-backup.vbs:

```
select case Weekday(BackupDate)
          'Please change your schedule here if necessary
          case vbSunday
                    Call BackupFull
          case vbMonday
                    Call BackupDiff
          case vbTuesday
                    Call BackupDiff
          case vbWednesday
                    Call BackupDiff
          case vbThursday
                    Call BackupDiff
          case vbFriday
                    Call BackupDiff
          case vbSaturday
                    Call BackupDiff
end select
```

Notes: Please ensure that the initial backup performed is set as BackupFull.

7. Save the changes in sps2k7-backup.vbs

8. Create the directory D:\BackupDir

9. Open the AhsayOBM console, create a file backup set for the SharePoint backup under the AhsayOBM console

10. Select the directory D:\BackupDir as Backup Source of the SharePoint backup set

11. Accept the default encryption settings by pressing the [OK] button if no change is necessary

12. Select the SharePoint backup set in the [Backup Setting] menu, select the [Command Line Tool]

13. Press the [Add] button under the Pre-Backup section on the right panel

14. Press the [Add] button under the Pre-Backup section on the right panel, enter the following entries in the corresponding text fields:

Example:
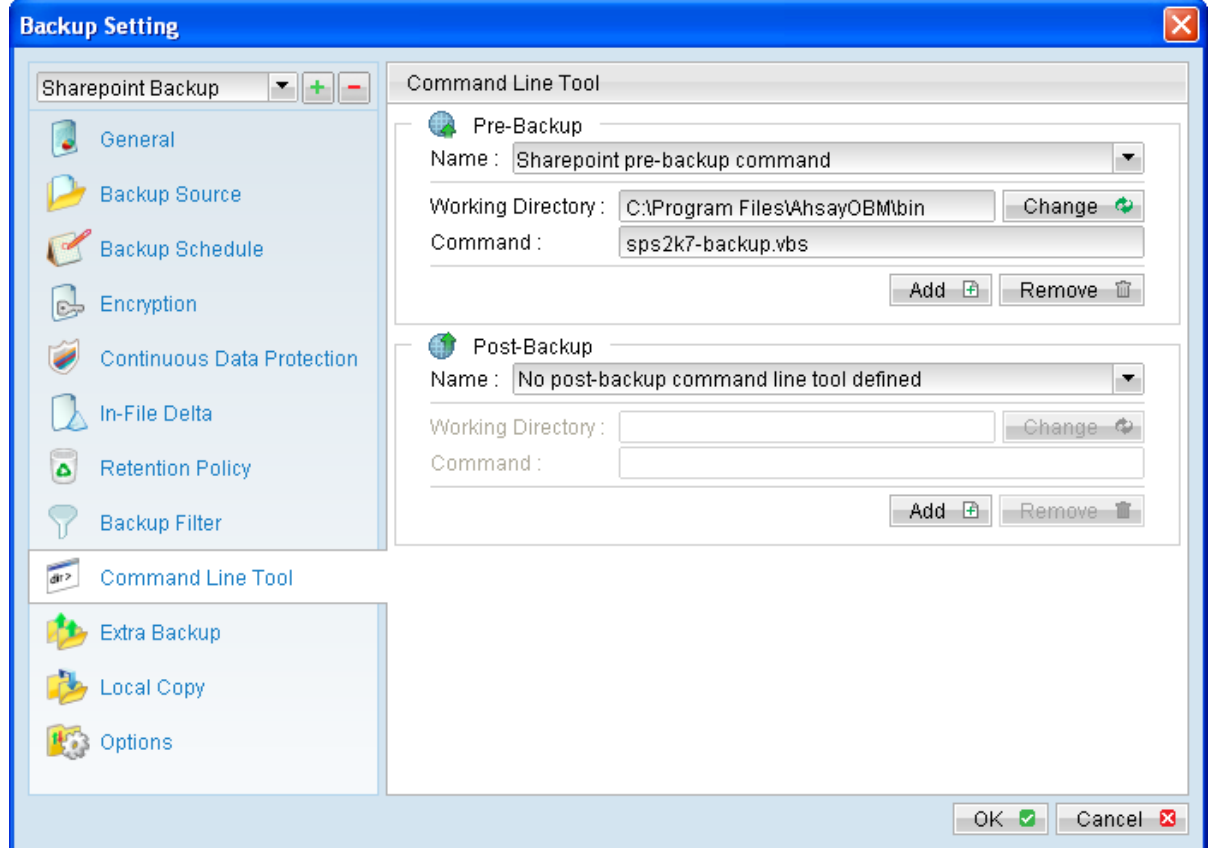
15. Press the [OK] button to save this setting

    The Windows SharePoint Services 2007 server can now be backed up by pressing the [Backup] button on the AhsayOBM console.

1.32 How do I restore SharePoint 2007 with AhsayOBM?

To restore your Windows SharePoint Services 2007 with AhsayOBM, please follow the instructions below:

1. Open the AhsayOBM console

2. Open the Restore page by selecting the [Restore] button on the AhsayOBM console

3. Select the SharePoint backup set from the backup set list, and browse to the backup directory

Example with the backup.dat file located in D:\BackupDir:
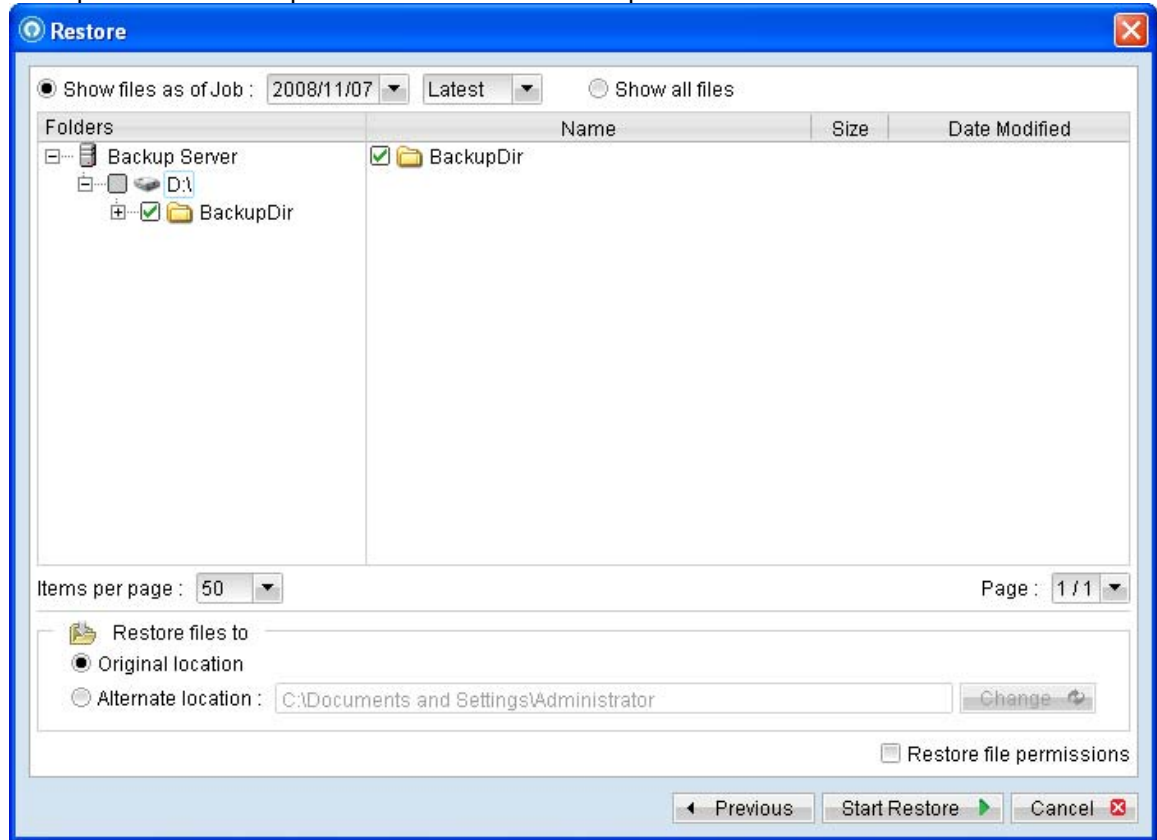
4. Select the checkbox next to the backup.dat node and press [Start Restore]

5. Login to the Sharepoint Central Administration page

6. Select the [Operations] tab from the top menu

7. Locate the [Restore from backup] link under the [Backup and Restore] section and select it

8. Enter D:\BackupDir in [Backup location] text field provided and press [OK]

9. Select the backup snapshot to be restored by selecting the radio button and select [Continue Restore Process]

10. Select the backup components to be restored by checking the desired checkboxes and select [Continue Restore Process] link

11. Select the desired [Restore Options] radio button option

12. Press the [OK] button to start the Sharepoint 2007 restoration process

    Notes:
    You are advised to check if the Sharepoint services are running properly before and after restoration. You can verify this by using the Sharepoint Central Administration page, select [Operations] and then the [Services on server] link under the [Topology and Services] section.

1.33 Can AhsayOBM be used to perform bare metal backup / restore?

Yes, Ahsay has integrated with StorageCraft's ShadowProtect and Windows 2008's backup utility (wbadmin) to provide bare metal backup / restore:

- ShadowProtect System Backup
- MS Windows System Backup

These two features for bare metal backup / restore are available for AhsayOBM version above 5.5.3.0.

Notes:

Operating System	Bit	ShadowProtect System Backup	MS Windows System Backup
Windows 2000 Professional / Server	32 Bit	✓	
Windows XP Home / Professional	32 / 64Bit	✓	
Windows Server 2003 Standard / Enterprise / Datacenter	32 / 64 Bit	✓	
Windows Server 2003 R2 Standard / Enterprise / Datacenter	32 / 64 Bit	✓	
Windows Vista Home	32 / 64 Bit	✓	
Windows Vista Business / Ultimate	32 / 64 Bit	✓	✓
Windows Server 2008 Standard / Enterprise / Datacenter	32 / 64 Bit	✓	✓

1.34 Factors affecting backup speed?

Stages of a backup job (initialized via AhsayOBM / AhsayACB or web interface) are outlined below:

1. A connection from the AhsayOBM client to the AhsayOBS server is established
2. Pre-command is run (if necessary)
3. A Shadow Copy set of the backup source is created (if available)
4. Download the server file list from the AhsayOBS server
5. Data of the backup source is compared with the server file list to compile the following file lists:

    i.   New file list
    ii. Modified file list
    iii. Deleted file list

6. Delta file is generated (if necessary)
7. Data are encrypted, compressed, and then uploaded onto the AhsayOBS server
8. The Shadow Copy set of the backup source is removed (if necessary)
9. Post-command is run (if necessary)
10. Backup is declared completed successful

Example with a backup job that is initialized via AhsayOBM:

Backup performance:
The following describes the factors that can affect the speed of a backup at different stages of the job:

1. Internet connection speed:

   i. Check on the speed of the connection between the AhsayOBM / AhsayACB client and the AhsayOBS server

   ii. Check if the backup job is being performed over a Local Area Network (LAN) or a Wide Area Network (WAN) environment

2. Hardware specification of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine:

   i. Check on the hardware specification of the machines in concern (RAM available, processor speed), are the resource sufficient for the backup operation

   ii. Check if the CPU usage is high during the restoration

   For machine installed on Windows, you can view the CPU usage with the Windows Task Manager
   For machine installed on Linux / Mac OS X, you can view the CPU usage with the command:

   Example:
   >top

   If the CPU usage is constantly maxed out during the restoration, it may suggest that the CPU power of the machine is insufficient for the backup operation

3. Disk specification of the disk of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine (network / local disk, SAN, NAS):

 i. For AhsayOBS with User Home that reside locally:

  a. Check on the local disk I/O performance of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine

  b. Check on the local disk I/O utilization of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine

  For machine installed on Windows, you can view the I/O utilization with the Windows Performance Monitor

  For machine installed on Linux / Mac OS X, you could view the I/O utilization with the command:

  Example:
  >iostat 1

  or

  >vmstat 1

  If the iostat tool is not installed, you can do so with the command:

  Example:
  >yum install sysstat

  If the I/O utilization of the disk in concern is high during the backup, please consider performing the backup job a an alternate time.

  Notes:
  The commands above will only works for machine with local partition.

 ii. For AhsayOBS with User Home that reside externally:

  a. Check on the I/O performance of the Network Attached Storage (NAS) or Storage Area Network (SAN)

  b. Check on the I/O utilization of the Network Attached Storage (NAS) or Storage Area Network (SAN)

4. Location of the backup source (local / network drive):

 i. Check if the backup source is located locally, or over a network

  If the backup source of the backup job is set over a network, the backup speed may be affected depending on the network traffic.

5. Location of the temporary directory (local / network drive):

 i. Check if the temporary directory specified for the backup set is located locally, or over a network

  If the temporary directory is specified on a network partition, the backup speed may be affected for backup type such as MS Exchange server backup, or MS SQL, depending on the network traffic.

6. Backup source data size (number of files and size of files):

    i.   How many files are selected as the backup source

    ii.   Check if the backup source contains a large number of files within a small number of directories

          If the size of the backup source is large, you may need to alter the amount of memory available to AhsayOBM. Please refer to Step 10 for more information.

7.   Number of delta to be generated:

    i.   How many delta files are being generated, and their size

          The speed of a backup job can be affected if the number to delta files to be generated is large, or if the delta files to be generated is large.

8.   Encryption setting:

    i.   Check on encryption key length configured for the backup set in concern

          For AhsayOBM / AhsayACB version after 5.5, backup data can be encrypted with key length of 256-bit, which may slow down the backup operation for machines with insufficient resource

9.   Local Copy module:

    i.   Check if the Local Copy module has been enabled for the backup set

          For AhsayOBM version after 5.5, local backup data are compressed and encrypted, which may also slow down the backup operation for machines with insufficient resource.

    ii.   Check if the Local Copy destination is located locally, or over a network (local / network drive)

          If the Local Copy destination of the backup job is configured to a network partition, the backup speed may be affected depending on the network traffic.

10. Amount of memory (Java heap size) available:

    i.   Check on the Java heap size setting, modify the setting if the currently allocated size is insufficient for the backup operation

          The instructions to modify the Java heap size can be found by Clicking Here.

11. Number of backup / restore job connecting to the AhsayOBS server:

    i.   Check on the number of backup / restore job connected to the AhsayOBS during the restoration

          If a high number of backup / restore job is connected to the AhsayOBS server during the backup operation, please consider performing the backup at another time.

12. Number of system routine job running on the AhsayOBS server:

    i.   Check on the number of resource intensive system job that is running when the backup job is performed (e.g. Rebuild User Storage, Cyclic Redundancy Check (CRC) Checking)

          If a high number of resource intensive system job is running when the backup job is performed, please consider performing the backup at another time.

1.35 Factors affecting restore speed?

Stages of a restore job (initialized via AhsayOBM / AhsayACB or web interface) are outlined below:

1. A connection from the AhsayOBM client to the AhsayOBS server is established
2. Download the restore file list from the AhsayOBS server
3. Create the directory path for the restoration (if necessary)
4. Download the backup data from the AhsayOBS server
5. All the data will be decompressed and decrypted on the AhsayOBM client side
6. Merging of delta files (if necessary)
7. Merging of combined delta file with full file
8. Restore is declared completed successful

Example with a restore job that is initialized via AhsayOBM:
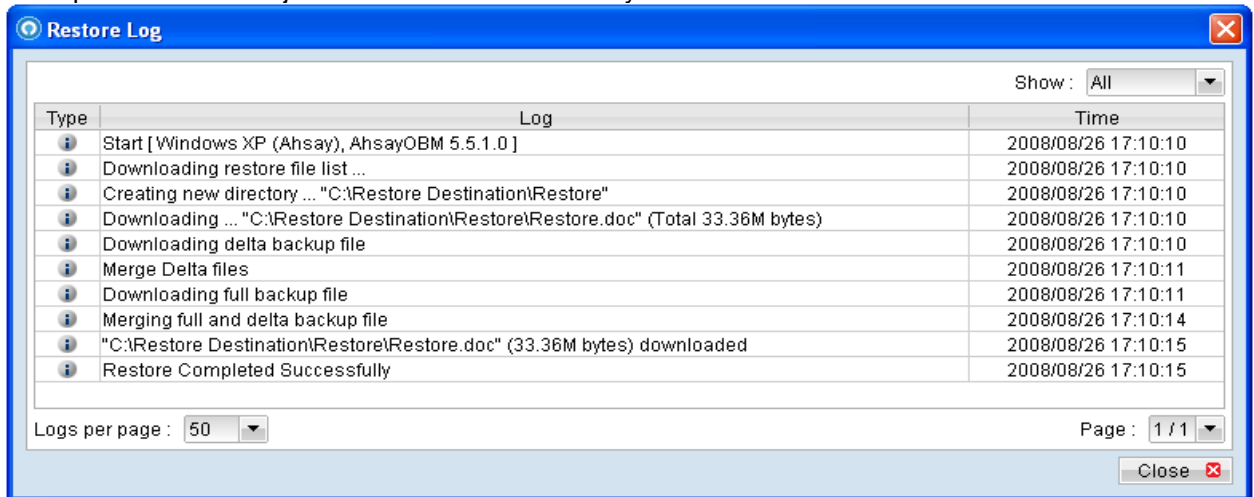
Restore performance:
The following describes the factors that can affect the speed of a restore at different stages of the job:

1. Internet connection speed:

    i. Check on the speed of the connection between the AhsayOBM / AhsayACB client and the AhsayOBS server

    ii. Check if the restore job is being performed over a Local Area Network (LAN) or a Wide Area Network (WAN) environment

2. Hardware specification of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine:

    i. Check on the hardware specification of the machines in concern (RAM available, processor speed), are the resource sufficient for the restore operation

    ii. Check if the CPU usage is high during the restoration

        For machine installed on Windows, you can view the CPU usage with the Windows Task Manager
        For machine installed on Linux / Mac OS X, you can view the CPU usage with the command:

        Example:
        >top

If the CPU usage is constantly maxed out during the restoration, it may suggest that the CPU power of the machine is insufficient for the restore operation

3. Disk specification of the disk of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine (network / local disk, SAN, NAS):

    i.   For AhsayOBS with User Home that reside locally:

        a. Check on the local disk I/O performance of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine

        b. Check on the local disk I/O utilization of the AhsayOBM / AhsayACB client machine, as well as the AhsayOBS server machine

           For machine installed on Windows, you can view the I/O utilization with the Windows Performance Monitor

           For machine installed on Linux / Mac OS X, you could view the I/O utilization with the command:

           Example:
           >iostat 1

           or

           >vmstat 1

           If the iostat tool is not installed, you can do so with the command:

           Example:
           >yum install sysstat

           If the I/O utilization of the disk in concern is high during the restoration, please consider performing the restore job a an alternate time.

           Notes:
           The commands above will only works for machine with local partition.

    ii.   For AhsayOBS with User Home that reside externally:

        a. Check on the I/O performance of the Network Attached Storage (NAS) or Storage Area Network (SAN)

        b. Check on the I/O utilization of the Network Attached Storage (NAS) or Storage Area Network (SAN)

4. Restore source data size (number of files and size of files):

    i.   How many files are selected as the restore source

    ii.   Check if the restore source contains a large number of files within a small number of directories

          If the size of the restore source is large, you may need to alter the amount of memory available to AhsayOBM. Please refer to Step 7 for more information.

5. Number of delta to be merged:

    i.   How many delta files are being merged

          Delta merging is a resource intensive procedure. Thus, the speed of a restore can be

greatly affected if the number to delta files to be merged is large

6. Java version (if the restore job has been initialized via the web interface):

   i. Check on the Java JRE version installed on the client machine

       For performance issue with web restore, you should consider upgrading the Java JRE version installed on the corresponding machine.

7. Amount of memory (Java heap size) available:

   i. Check on the Java heap size setting, modify the setting if the currently allocated size is insufficient for the restore operation

       The instructions to modify the Java heap size can be found by Clicking Here.

8. Location of the restore destination (network drive / local drive):

   i. Check if the restore destination of the restore job is configured to a network or local partition

       If the restore destination of the restore job is set over a network, the restore speed may be affected depending on the network traffic.

9. Number of backup / restore job connecting to the AhsayOBS server:

   i. Check on the number of backup / restore job connected to the AhsayOBS during the restoration

       If a high number of backup / restore job is connected to the AhsayOBS server during the restore operation, please consider performing the restore at another time.

10. Number of system routine job running on the AhsayOBS server:

    i. Check on the number of resource intensive system job that is running when the backup job is performed (e.g. Rebuild User Storage, Cyclic Redundancy Check (CRC) Checking)

        If a high number of resource intensive system job is running when the restoration is performed, please consider performing the restore at another time.

1.36 Where can I find the client log on a AhsayOBM / AhsayACB client machine?

This document contains the information of where the client log can be located.

The client log on a AhsayOBM client machine can be found under the following directories:

Windows 2000, XP, 2003:

- C:\Documents and Settings\Administrator\.obm\log
- C:\Program Files\AhsayOBM\log
- C:\Program Files\AhsayOBM\AUA\log
- C:\Documents and Settings\All Users\Application Data\AhsayOBM\CDP\log

Windows Vista:

- C:\Users\Administrator\.obm\log
- C:\Program Files\AhsayOBM\log

- C:\Program Files\AhsayOBM\AUA\log
- C:\Users\All Users\AhsayOBM\CDP\log

Linux / Unix:

- ~/.obm/log & /usr/local/obm/log
- /usr/local/obm/aua/log

Mac OS X:

- ~/.obm/log & /Applications/AhsayOBM/log
- /Applications/AhsayOBM/aua/log

The client log on a AhsayACB client machine can be found under the following directories:

Windows 2000, XP, 2003:

- C:\Documents and Settings\administrator\.acb\log
- C:\Program Files\AhsayACB\log
- C:\Program Files\AhsayACB\AUA\log
- C:\Documents and Settings\All Users\Application Data\AhsayACB\CDP\log

Windows Vista:

- C:\Users\administrator\.acb\log
- C:\Program Files\AhsayACB\log
- C:\Program Files\AhsayACB\AUA\log
- C:\Users\All Users\AhsayACB\CDP\log

Mac OS X:

- ~/.acb/log & /Applications/AhsayACB/log
- /Applications/AhsayACB/aua/log

1.37 Pre and post-backup command to close and open Microsoft Outlook?

Yes, you can try the pre-backup command similar to the example as shown below:

Example:
TASKLIST | FIND "OUTLOOK.EXE"
if errorlevel 1 goto end
if errorlevel 0 taskkill /im outlook.exe /F
:end

Save the commands above in the file called CloseOutlook.cmd, and then specify the corresponding working directory and command in the Command Line Tool module.

Example in AhsayOBM:
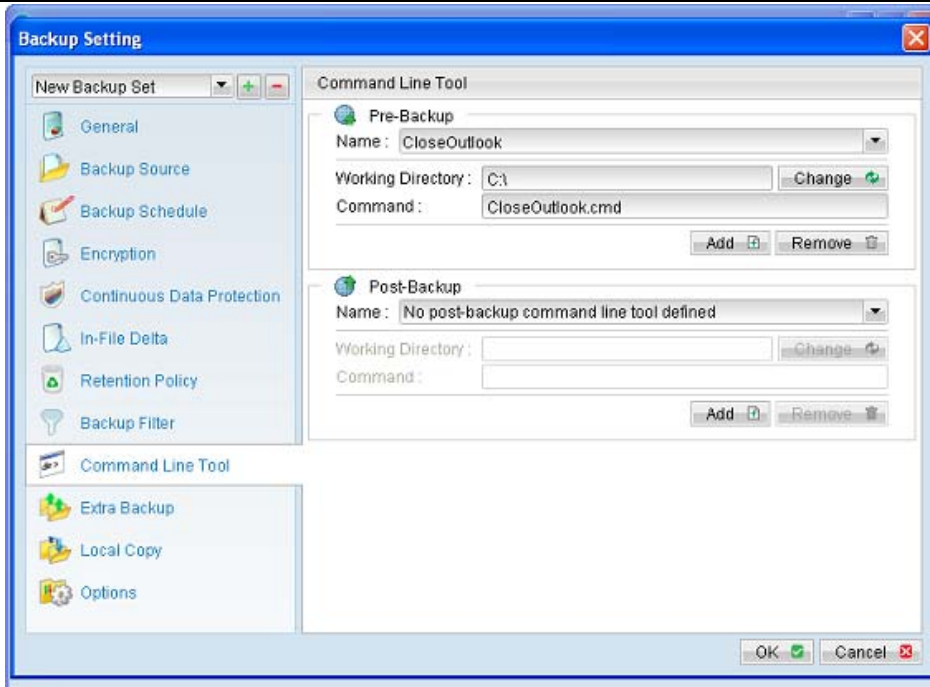
You can also open the Microsoft Outlook application after the backup job has been completed. To do so, you can try the post-backup command similar to the example as show below:

Example:
${PATH}\Outlook.lnk
exit

Where PATH is the directory path to the Outlook shortcut. Save the commands above in the file called OpenOutlook.cmd, and then specify the corresponding working directory and command in the Command Line Tool module.

Example in AhsayOBM:
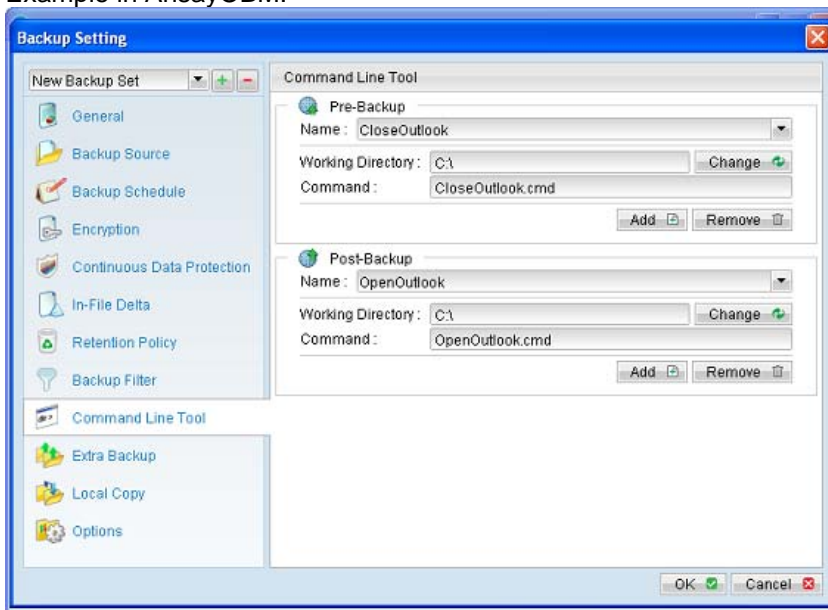
You can also select to open Outlook in normal window, minimized mode or maximized mode by editing

the properties of the shortcut file. Example:
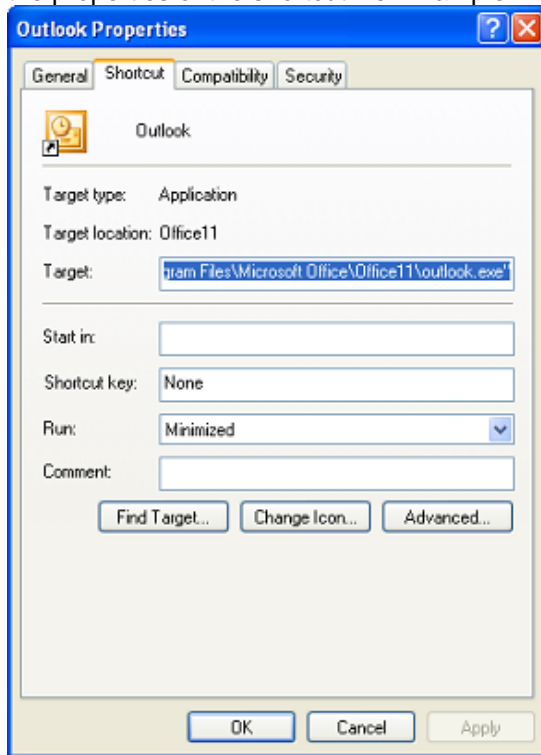
1.38 Post-command to shutdown the machine after a backup job is completed?

Yes, you can try the post-command similar to the example as shown below:

Example:
SHUTDOWN -s -t 60
Save the commands above in the Post-Backup command field, and then specify the corresponding working directory to C:\.

Example in AhsayOBM:
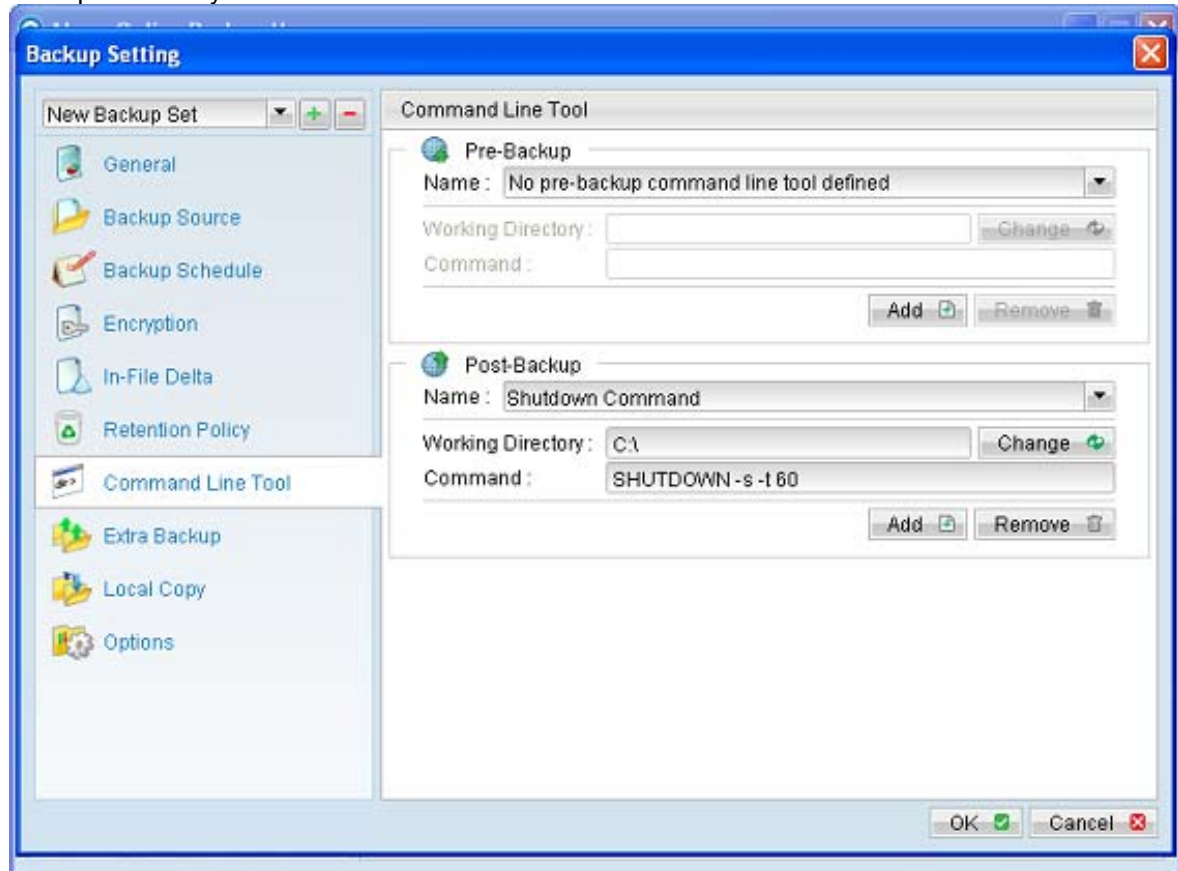
For more details on the SHUTDOWN command:

SHUTDOWN [-l[1] | -s[2] | -r[3]] [-t xx[4]] [-c "comment"[5]]

[1] The -l option specifies system log out
[2] The -s option specifies system shutdown
[3] The -r option specifies system restart
[4] The -t option specifies timeout for shutdown to xx seconds
[5] The -c option specifies shutdown comment (maximum of 127 characters)

1.39 How do I migrate backup source of an existing backup set without re-uploading the data?

This document contains the information of how to migrate backup source of an existing backup set without re-uploading the data.

Assumptions:
You want to migrate backup source from

C:\Backup_Source (e.g. the directory of where the data currently reside)

to

D:\Backup_Source (e.g. the new directory of where the data will be migrated to)

Notes:
The following procedure is only necessary for backup source migration between different root drive, or if the "top-most" directory of the backup source have changed.

For movement of data within the backup source, AhsayOBM / AhsayACB would automatically detected the data as moved file, and no user action is required.

Instructions:
Please refer to the following instructions:

1. On the corresponding client machine, create an empty directory "D:\Backup_Source" prior to the migration of data

Notes:
It is important that Step 1 is performed before the migration of the data. If not, the data will be considered as new data, and AhsayOBM / AhsayACB will re-upload the data when the next backup job is performed.

2. Open the AhsayOBM console, select the corresponding backup set

3. Add the newly created directory "D:\Backup_Source" to the backup source of the corresponding backup set:
    Example:
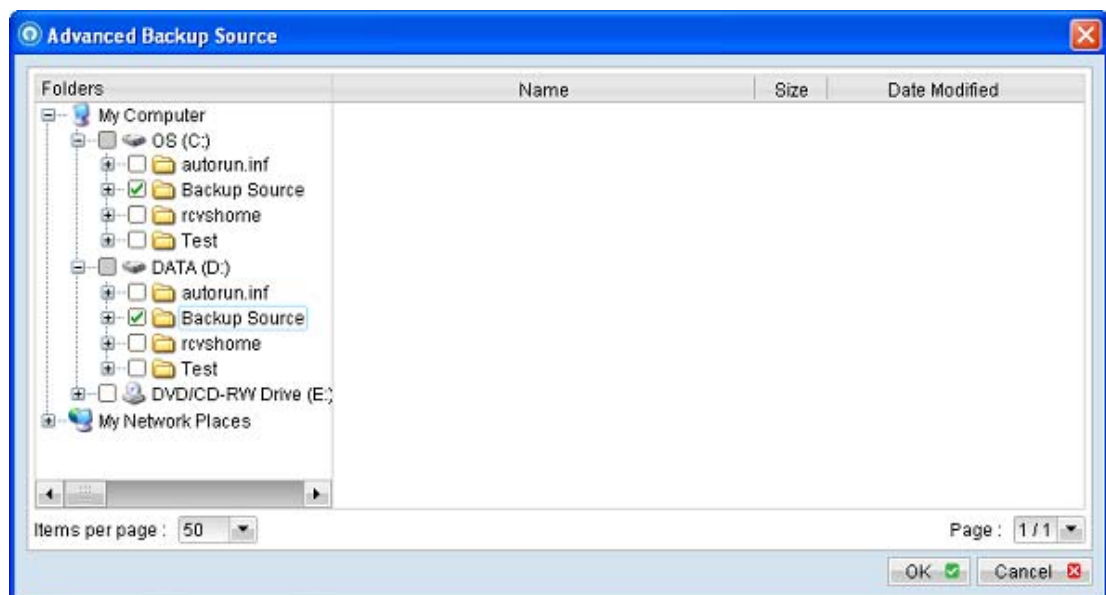
Notes:
For AhsayOBM / AhsayACB installation on Linux, you can add the newly created directory to the backup source of the corresponding backup set via the AhsayOBS management console.

4. Press the [OK], and [Save Setting] button to save this setting

5. Perform the backup job, and press the [Quit] button to exit AhsayOBM

6. On the corresponding client machine, move the data from:

   C:\Backup_Source

   to

   D:\Backup_Source

7. Perform the backup job again afterward

Notes:
For AhsayOBM / AhsayACB installation on Linux, the basic concept is the same, except that all directory paths are in the Linux convention

1.40 How do I manually stop a scheduled backup that is running?

To stop a scheduled backup that is running on Mac OS X, please follow the instruction below:

1. Please open a terminal window
2. Enter the command:

   Example:
   >touch ~/.obm/ipc/BackupSet/Backup_ID/stop

For backup job that is running on other platforms, simply create a file call "stop" within the ipc folder. The ipc folder can be found at the following directory path:

For Windows 2000, XP, 2003:
    C:\Documents and Settings\Administrator\.obm\ipc\BackupSet\Backup_ID

For Windows Vista, 2008, 7:
    C:\Users\Administrator\.obm\ipc\BackupSet\Backup_ID

For Linux / Unix:
    ~/.obm/log/ipc/BackupSet/Backup_ID

2 Common Error Messages

2.1 The process cannot access the file because it is being used by another process

When performing a file backup, the following error message is received:

[Error][Updated File] File="\\Network_Path\Directory\File" Error="The process cannot access the file because another process has locked a portion of the file."

The message suggests that the corresponding file is locked by other application when the backup job is performed.

In this case, although the AhsayOBM / AhsayACB user may have Volume Shadow Copy enabled. However, since the file in use resides on a network area, thus a Shadow Copy of the file cannot be created.

To resolve the issue, please close the application which is accessing the file before performing the backup.

2.2 Cannot write to C:\TEMP (web restore on Internet Explorer 7 with Protected Mode on)

When performing a web restore, the following error message is received in the Online Backup File Restoring Manager or the Internet Explorer 7 web browser may stop responding:

Example: [YYYY-MM-DD hh:mm:ss] "Cannot write to \DIRECTORY"
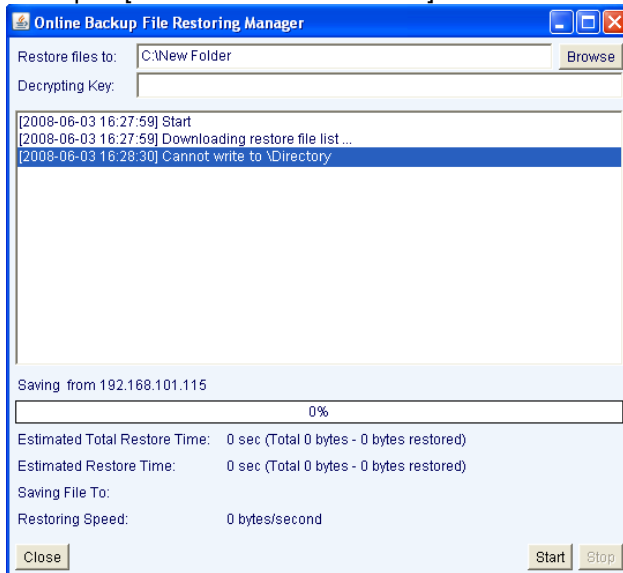
The problem will usually occur when Internet Explorer 7 is running in Protected Mode (a new feature only applied on Windows Vista).

To resolve the issue, please verify if the problematic machine is running on Windows Vista with Internet Explorer 7. If yes, please also verify if the Internet Explorer 7 is running in "Protected Mode".

This can be done by viewing the bottom right of Internet Explorer 7: "Protected Mode:On" or "Protected Mode:Off".

Example:
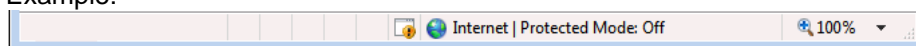
If the option is turned on, please disable it by selecting: Tools -> Internet Options -> Security , select the

appropriate zone, and uncheck the option "Enable Protected Mode".

Example: Tools -> Internet Options -> Security
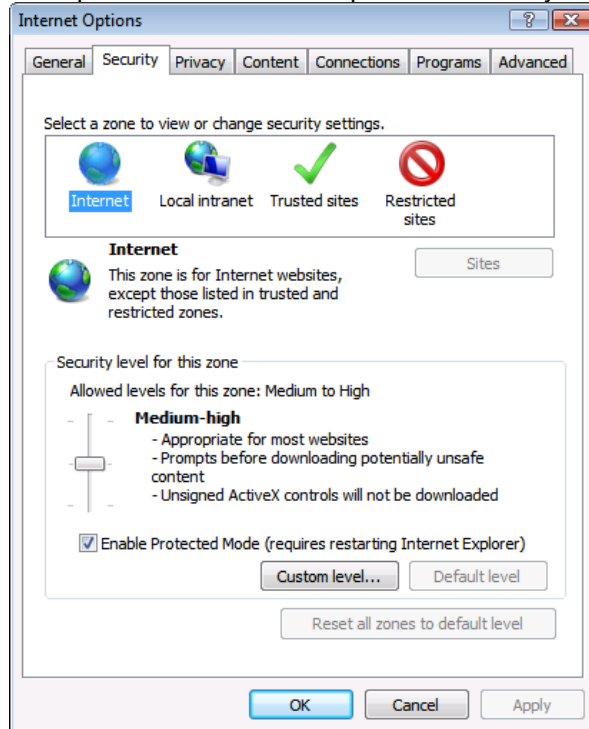
In the cases where the problem persist, please also disable the User Account Control (UAC) on the affected machine.

You could do so by selecting Control Panel, type in "UAC" in the search box, and then select "Turn User Account Control (UAC) on or off". On the next screen, uncheck the "Use User Account Control (UAC)" option, and then click "OK".

If required, you may enable the the Protect Mode of Internet Explorer, and the UAC on the affected machine after the web restore has been completed. Alternatively, you could also perform the web restore using other web browser such as Mozilla Firefox or Opera.

2.3 Backup job that is scheduled to be performed is not starting (missed backup)?

Backup job that is scheduled to be performed is not starting? How can we troubleshoot for the cause of the issue?

Outlined below are some guidelines on how to troubleshoot the issue:

1. Please verify if the affected machine is switched off, hibernated or in standby mode when the scheduled backup is due to run.

2. Please ensure that the "Run scheduled backup on computers named" for the backup set has been populated properly:

    Example:

    This field is introduced in AhsayOBS version 5.2 to assure that one backup set can only be run on one computer, making multiple computer backup using a single backup account more robust.

    If you see a question mark '?' for the "Run scheduled backup on computers named" field, please patch the AhsayOBS software to the latest patch release. The instruction can be found by Clicking

Here.

After that, enter correct values for the "Run scheduled backup on computers named" for those problematic backup set.

3. If the affected client is on AhsayOBM / AhsayACB version 5.2.1.0 and scheduled backup jobs are usually missed after the server is rebooted, please verify on the info.log.

The info.log is located in:

AhsayOBM:
(Windows)   C:\Program Files\AhsayOBM\ipc\Scheduler
(Linux)   /usr/local/obm/ipc/Scheduler
(Mac OS X)   /Applications/AhsayOBM/ipc/Scheduler

AhsayACB:
(Windows)   C:\Program Files\AhsayACB\ipc\Scheduler
(Mac OS X)   /Applications/AhsayACB/ipc/Scheduler

Verify if there are entries similar to the example below:

[YYYY/MM/DD hh:mm:ss] Scheduler Version=5.2.1.0
[YYYY/MM/DD hh:mm:ss] Java Vendor=Sun Microsystems Inc. Version=1.4.2_10
[YYYY/MM/DD hh:mm:ss] [info] Starting Scheduler, User:'Username', Home:'C:\Documents and Settings\Username\.obm'
[YYYY/MM/DD hh:mm:ss] Another Scheduler is running! This Scheduler will not start!

To get the scheduler running again, you need to remove a file called "running" which reside in the folder ${Install-Home}\ipc\Scheduler\ and then restart the [Online Backup Scheduler] service.

To permanently resolve the issue, please also patch the AhsayOBM / AhsayACB software to the latest patch release. The instruction can be found by Clicking Here.

4. Verify if the home.txt has been populated correctly. The home.txt is located in:

AhsayOBM:
(Windows)   C:\Program Files\AhsayOBM
(Linux)   /usr/local/obm
(Mac OS X)   /Applications/AhsayOBM

AhsayACB:
(Windows)   C:\Program Files\AhsayACB
(Mac OS X)   /Applications/AhsayACB

You should see at least one entry pointing to a .obm (or .acb) folder that is accessible by the local scheduler service, for example "C:\Documents and Settings\administrator\.obm". Please modify the home.txt file if this is not the case.

5. Check if the scheduler service is running by inspecting the client side scheduler log. The scheduler debug log is located in:

AhsayOBM:
(Windows)   C:\Documents and Settings\administrator\.obm\log\Scheduler\debug.log
(Linux)   ~/.obm/log/Scheduler/debug.log
(Mac OS X)   ~/.obm/log/Scheduler/debug.log

AhsayACB:
(Windows)   C:\Documents and Settings\administrator\.acb\log\Scheduler\debug.log
(Mac OS X)   ~/.acb/log/Scheduler/debug.log

This log contains every detail on the scheduler service.

If the schedule is working fine, the client side scheduler log should contain entries similar to the following example:

[YYYY/MM/DD hh:mm:ss][info][Thread][Reloader] Loading profile from server ...
[YYYY/MM/DD hh:mm:ss][info][LocalProfile.loadFromServer] Loading profile from server ...
[YYYY/MM/DD hh:mm:ss][info][LocalProfile.loadFromServer] Loaded profile from server.
[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Next backup will run in 0 hr 36 min 37 sec
[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Next backup will run in 80 hr 16 min 37 sec
[YYYY/MM/DD hh:mm:ss][info][Thread][Reloader] Loaded profile from server.

Otherwise, please restart the scheduler service. If the problem persists, please consider re-installing the AhsayOBM / AhsayACB software or the scheduler service.

If the AhsayOBM / AhsayACB software is installed on a Windows 2000 machine, the scheduler service can stall at times due to the instability of Windows 2000's Services. A workaround is to write a batch job that restart the scheduler service periodically.

Please also check whether entries similar to the following example can be found at the scheduled backup time:

[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Wake Up ...
[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] This backup job will run to its completion.
[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Start running backup

Otherwise, if there is error message found, please contact our Support Engineer with details of the situation.

6. If the AhsayOBM software is installed on a Linux machine, please try running the Configurator.sh script to set appropriate backup account and password.

7. If the affected client is on AhsayOBM / AhsayACB version Post-5.2.6.3, please verify whether entries similar to the following example can be found at the client side scheduler log:

[YYYY/MM/DD hh:mm:ss][info][LocalProfile.loadFromServer] Loading profile from server ...
[YYYY/MM/DD hh:mm:ss][info][error][Scheduler.run] Cannot load profile from server. Retry in 300 seconds ... Error= '[SSLSocketJVM14.getSSLSocket] Hostname verifying failed!'. Still Fail After Retry!!!! ...
[YYYY/MM/DD hh:mm:ss][info] Scheduler stopped.

If there is, the problem is most likely related to the certificate installed on the AhsayOBS server. Instruction on how to resolve the issue can be found in Article #1627.

8. If the AhsayOBM software is installed on a Linux machine, and the version of the affected client is on Post-5.5.1.0, please verify whether entries similar to the following example can be found at the client side scheduler log:

[YYYY/MM/DD hh:mm:ss][info][Backup Set (Backup ID)] Start running backup
[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] Error: no `server
[YYYY/MM/DD hh:mm:ss][info][Backup Set (Backup ID)] Finished running backup
[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] ' JVM at
`/usr/local/obm/jvm/lib/i386/server
[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] /libjvm.so'.

If there is, the problem is most likely related to the Java package that is bundled with the AhsayOBM application. To resolve the issue, please refer to Article #2038.

9. If the backup type of the affected backup set is MS Exchange mail-level, and the affected client has just been upgraded from AhsayOBM version 5.2 to 5.5, please verify whether entries similar to the following example can be found at the client side scheduler log:

[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] 'ObmJW' is not recognized as an internal or external command,
[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] operable program or batch file.

or

[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] 'bJW' is not recognized as an internal or external command,
[YYYY/MM/DD hh:mm:ss][error][OBM.ErrorStream][Backup Set] operable program or batch file.

If there is, the problem is most likely related to the renaming of the ObmJW.exe file (for AhsayOBM version 5.2 to 5.5). To resolve the issue, please refer to Article #1932.

10. If the backup type of the affected backup set is MS Exchange mail-level, and the affected machine has any Windows Security Update patch released after 16-04-2009 installed, please verify whether entries similar to the following example can be found at the client side scheduler log:

[YYYY/MM/DD hh:mm:ss][info][OBM.OutputStream][Backup Set] Error occurred during initialization of VM
[YYYY/MM/DD hh:mm:ss][info][OBM.OutputStream][Backup Set] Could not reserve enough space for object heap

If there is, the problem is most likely related to insufficient physical memory. To resolve the issue, please refer to Article #2112.

11. Please verify whether entries similar to the following example could be found at the client side scheduler log:

[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Next backup will run in 0 hr 1 min 0 sec
[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Skipping scheduled backup on this computer. Schedule should run on machine_a, current computer name:machine_b

When a scheduled backup is due to run, the scheduler service will first verify if the machine found on the machine is the same as the machine name specified in the backup set setting (please refer to Step 2 above). If the machine of the affected machine has changed, the scheduled backup job will be skipped by the scheduler service, because the machine name cannot be matched.

To resolve the issue, please ensure that the scheduled backups on the corresponding machine is configured properly, please make sure that the correct machine name has been set in the AhsayOBS management console for the relevant backup set. Under [Manage System]- > [Manage User] -> [Username] -> [Backup Set] -> [Run scheduled backup on computers named].

12. If the AhsayOBM / AhsayACB software is installed on a Mac OS X machine, and the hostname of the affected machine is often changed due to different DHCP server assignment (user who travel often with MacBook). Please verify whether entries similar to the following example could be found at the client side scheduler log:

[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Next backup will run in 0 hr 1 min 0 sec
[YYYY/MM/DD hh:mm:ss][info][BackupSet (Backup_ID)] Skipping scheduled backup on this computer. Schedule should run on hostname_a, current computer name:hostname_b

When a scheduled backup is due to run, the scheduler service will first verify if the hostname found on the machine is the same as the hostname / machine name specified in the backup set setting (please refer to Step 2 above). If the hostname of the affected machine has changed, the scheduled backup job will actually be skipped by the scheduler service, because the hostname cannot be matched.

To resolve the issue, please follow the instructions as follow:

    i.   Open a terminal
    ii.   Enter the command "sudo vi /etc/hostconfig"

     iii.   Add the following entry "HOSTNAME={%YOUR MACHINE NAME%} into the /etc/hostconfig file

     iv.   Reboot the machine

After the machine has been restarted:

     v.   Open a terminal

     vi.   Use the "hostname" command to obtain the hostname of the machine, it should now return the machine name you have specified

Then connect the affected machine to another DHCP network, using the "hostname" command should return your preset hostname

Finally, to ensure that scheduled backups on are configured properly, please make sure that the correct hostname has been set in the AhsayOBS management console for the relevant backup set. Under [Manage System]- > [Manage User] -> [Username] -> [Backup Set] -> [Run scheduled backup on computers named].

13. If the AhsayOBM / AhsayACB software is installed on a Mac OS X machine, please also verify in the console.log if there is any error message found. The console.log file can be found in:

AhsayOBM:
/Applications/Ahsay Online Backup Manager/log/Scheduler

AhsayACB:
/Applications/Ahsay A-Click Backup

14. If you are still having problem, please contact our Support Engineer with details of the situation.
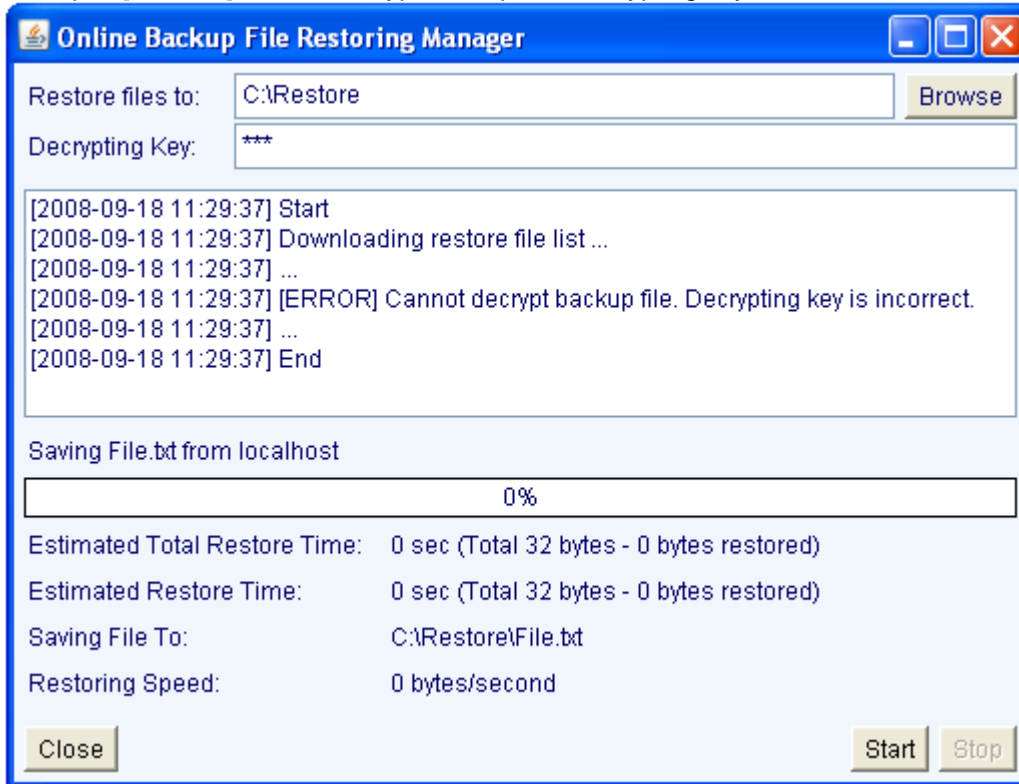
Notes:
We would just like to clarify that missed backup may not necessarily be problem. End-users may have their PC/server switched off, hibernated or in standby mode when the schedule is due to run, or network can be unavailable or being cut off during the scheduled backup time. We have also seen cases where the system clocks of the client machine and that of AhsayOBS are off.

2.4 Encrypting key entered is not accepted?

When performing a web restore, the following error message is received in the Online Backup Fle Restoring Manager:

Example: [ERROR] Cannot decrypt backup file. Decrypting key is incorrect

```
Online Backup File Restoring Manager

Restore files to:     C:\Restore                               Browse

Decrypting Key:       ***

[2008-09-18 11:29:37] Start
[2008-09-18 11:29:37] Downloading restore file list ...
[2008-09-18 11:29:37] ...
[2008-09-18 11:29:37] [ERROR] Cannot decrypt backup file. Decrypting key is incorrect.
[2008-09-18 11:29:37] ...
[2008-09-18 11:29:37] End

Saving File.txt from localhost

                                 0%

Estimated Total Restore Time:   0 sec (Total 32 bytes - 0 bytes restored)

Estimated Restore Time:         0 sec (Total 32 bytes - 0 bytes restored)

Saving File To:                 C:\Restore\File.txt

Restoring Speed:                0 bytes/second

Close                                               Start    Stop
```

or

When attempting to perform a restore using the backup client user interface, AhsayOBM / AhsayACB repeatedly prompted for a correct encrypting key.

Outlined below are some guidelines on how to troubleshoot the issue:

1. Please verify if the user had selected the Default encryption setting of "Use Login Password as Encrypting Key", or Custom (see Step 5 if Custom is selected)

2. If the Default encryption setting is selected, please verify if there was any password change(s) to the backup account in concern. In most cases, a change in the password would not lead to a change of encrypting key. However, there could be exceptional cases where:

    i.   The client has changed his/her password, and then login to AhsayOBM / AhsayACB (with the same backup account) on another machine
    ii. The client has changed his/her password, and the User Profile directory (e.g. C:\Documents and Settings\Administrator\.obm\config) had been removed, he/she then login to AhsayOBM / AhsayACB (with the same backup account)

    In the cases above, AhsayOBM will prompt for the encrypting key setting for the backup sets that existed with the account. At this time, if the user had changed his password, he should enter the original password as the encrypting key. If the user select "Use Login Password as Encrypting Key", data of this particular backup set will then contain two encrypting key:

    iii. In the cases where the encrypting key was changed, please perform the restore using the user's previous password(s)

  iv. In the cases where the previous encrypting key(s) is lost, there will be no way to restore data from the corresponding backup set

3. Please also verify if the user had triggered the "Forgotten Password" email via the web console, and then login to their AhsayOBM console using the hashed version of their password

4. Please perform the restore using the hashed version of the corresponding user's password (or hashed version of the user's previous password). To do so, please contact our Support Engineer with details of the situation

5. If Custom encryption setting is selected, the user must use the correct encrypting key to restore the data

6. Please verify if the restore destination has enough storage space for the restore operation

7. In the cases where the AhsayOBS server is installed on a Windows 2000 / XP machine, with User Home(s) configured to a network storage device. If the particular file from the restore source exceeded 4GB, the file may not be restorable due to Windows 2000/XP limitation. Please refer to the following URL for more information:

  http://support.microsoft.com/kb/898068/en-us

8. In the cases where the AhsayOBS server was upgraded from version 5.2 to 5.5. If the restorer applet file (obrA.jar) was copied from:

  %5.2_Install_Home%\webapps\obs\jsp\applet\obr\obrA.jar

  to

  %5.5_Install_Home%\webapps\obs\jsp\applet\obr\obrA.jar

  Data may not be restorable due to the new key length introduced for AhsayOBS version 5.5 (introduction of 256-bit key length for encryption). To resolve the issue, please replace the existing obrA.jar file with the latest obrA.jar file which can be obtained from the following URL:

  http://www.ahsay.com/en/service_providers/ahsay_service_providers_latest_version.html

  Notes:
  You need to install the latest version of AhsayOBS at a temporary location to obtain the obrA.jar file (e.g. %Temporary_Location%\webapps\obs\jsp\applet\obr\obrA.jar)

  For partners with signed restorer applet, you may need to re-sign the obrA.jar file with instructions provided by your Certification Authority (CA).

9. For AhsayOBM version 5.2, verify if the system account running AhsayOBM has sufficient permission to write on the restore destination.

10. As a last resort, please verify on the data integrity of the affected backup set

  You can do so by logging into AhsayOBS management console, and then select [Manage User] -> [User Profile], you shall see an option just under the user summary called [File Validation Option], clicking on this will display the options and a [Check] button. Please enable the [Verify Checksum] option, and click on the [Check] button to start the single user rebuild.

  When the Single User Storage Rebuild is started for the affected user, please verify if the following error message is received in the system log:

  [info][system][BackupSet.rebuildIndexDir] File 'User_Home\username\files\Backup_ID\YYYY-MM-DD-hh-mm-ss\File has incorrect checksum. It will be uploaded again in next backup.

If there is, the problem may be related to data integrity of the affected file(s). Since the file(s) is being referenced with an incorrect checksum, the integrity of these data is compromised, and they are not restorable.

Notes:
Once a file has been flagged as having incorrect checksum by the Single User Storage Rebuild job, the file will be purged when the next backup is performed.

2.5 The process cannot access the file ... (on Network Drive)

When performing a file backup, the following error message is received:

[Error][Updated File] File="\\Network_Path\Directory\File" Error="The process cannot access the file because another process has locked a portion of the file."

The message suggests that the corresponding file is locked by other application when the backup job is performed.

In this case, although the AhsayOBM / AhsayACB user may have Volume Shadow Copy enabled. However, since the file in use resides on a network area, thus a Shadow Copy of the file cannot be created.

To resolve the issue, please close the application which is accessing the file before performing the backup.

2.6 [BackupSet.append] Uploaded file size incorrect

When performing a backup of any type, the following error message is received in the backup report:

[BackupSet.append] Uploaded file size incorrect. File='\Directory_Path\File'
Location='User_Home\User\files\Backup_ID\Current\xxxx\xxxx\xxxx\xxxx\File' ExpectedFileSize=A
UploadedFileSize=B

or

File size incorrect (expected=A found=B). Deleting backup file -
    ServerPath='User_Home\User\files\Backup_ID\Current\xxxx\xxxx\xxxx\xxxx\File'
    BackupSet='Backup_Set(Backup_ID)' BackupJob='Current' ClientPath='Directory_Path\File'
    RunByBackupJob='YYYY-MM-DD-hh-mm-ss'

The message suggests that the AhsayOBS server detected a size difference between the file size received and the file size that it was expecting. Some possible causes of this issue can be network instability, packet drop, etc.

If the issue only occurs occasionally, you can safely ignore the error.

In the cases where the network between the AhsayOBS server and the AhsayOBM client remain unstable, you can try decreasing the transfer block size. You can do so by logging into your AhsayOBM console, select [Setting], and modify [Transfer Block Size].

In the cases where the AhsayOBS server is installed on a Windows 2000 or XP machine. If the file(s) in concern exceeded 4 GB, then the problem is actually related to limitation on the operating system itself. AhsayOBS that run on Windows 2000 or XP will have problem writing file(s) larger than 4 GB.

Since Windows does not return any write error, it misleaded AhsayOBS to determine that the file write is fine. Thus, the error "File size incorrect" would be returned on every subsequent backups.

To resolve the issue, please refer to the following URL: http://support.microsoft.com/kb/898068/en-us

2.7 [BackupSetFileSystem.resetNumDeltaMade] No full backup found for this checksum file

When performing a backup of any type, the following error message is received in the backup report:

[BackupSetFileSystem.resetNumDeltaMade] No full backup found for this checksum file. Job='Current' File='\Directory_Path\File'

The message suggests that the AhsayOBS server cannot locate the corresponding full file for one of the checksum file(s).

To resolve the issue, please rebuild the User Storage for the corresponding user in concern.

You can do so by logging into AhsayOBS management console, and then select [Manage User] -> [User Profile], you should see an option just under the user summary called [File Validation Option], clicking on this will display the options and a [Check] button. Enable the [Verify Checksum] option, and click on the [Check] button to start the single user rebuild.

Please allow the rebuild user storage job to run to its completion, and then perform a manual backup afterward.

Notes:
When the single user rebuild is completed, the user statistic of the corresponding user will be displayed in the system log. The system log can be found under the AhsayOBS management console: [Manage Log] -> [System Log]

2.8 [BackupSet.append] Checksum incorrect

When performing a backup of any type, the following error message is received in the backup report:

[BackupSet.append] Checksum incorrect. File='\Directory_Path\File'
Location='User_Home\Username\files\Backup_ID\Current\xxxx\xxxx\xxxx\xxxx\File' Recd=A Cald=B

The message suggests that the checksum file of the corresponding data on the AhsayOBS server is not correct.

To resolve the issue, please rebuild the User Storage for the corresponding user in concern.

You can do so by logging into AhsayOBS management console, and then select [Manage User] -> [User Profile], you should see an option just under the user summary called [File Validation Option], clicking on this will display the options and a [Check] button. Enable the [Verify Checksum] option, and click on the [Check] button to start the single user rebuild.

Please allow the rebuild user storage job to run to its completion, and then perform a manual backup afterward.

Notes:
When the single user rebuild is completed, the user statistic of the corresponding user will be displayed in the system log. The system log can be found under the AhsayOBS management console: [Manage Log] -> [System Log]

2.9 "\Directory_Path\File" has been removed already

When performing a file backup, the following informative message is received in the backup report.

"\Directory_Path\File" has been removed already

The message suggests that during the uploading stage of a backup job, the corresponding file(s) identified in the file comparison stage no longer exists on the client machine. This usually happens to temporary file(s) that is created and removed frequently.

To further explain, when a backup job is started, the following actions are performed by AhsayOBM.

1. Pre-command(s)
2. Create Volume Shadow Copy (if necessary)
3. Download the remote file list from the AhsayOBS server
4. Compare the local files with the remote file list determine the list of file(s) to be uploaded
5. Upload the data listed in Step 4
6. Post-command(s)
7. Remove the created Volume Shadow Copy

The message "...has been removed already" is flagged when a file(s) that was listed in the local file list (Step 4) no longer exists on the client machine in the file upload stage (Step 5).

Furthermore, this problem can also occurs if an incorrect Volume Shadow Copy snapshot of the file has been created, or if the affected file is not included in the Volume Shadow Copy snapshot.

Finally, for AhsayOBM / AhsayACB version prior to 5.5.1.0, this issue can also occurs if the "Temporary directory for storing backup files" assigned for the affected backup set has been set to a directory that does not exist.

To resolve the issue, please follow the instructions below:

If In-file delta is enabled for the backup set in concern, please ensure that the "Temporary directory for storing backup files" setting of AhsayOBM is set to a writable directory with sufficient disk space.

Please also verify if the file(s) in concern is temporary file. If it is, please un-select these files from the backup source to resolve the issue.

In the cases where the issue is caused by incorrect snapshot of Volume Shadow Copy, please follow the instructions below:

Windows XP / Vista:
To resolve the issue, please re-register the Volume Shadow Copy Service. To do so, you could utilize the "RegisterVSS.bat" script available in ${Install-Home}\bin. Please also reboot the machine afterward.

Notes:
Please safely ignore the error message(s) displayed during the re-registration, as some of the DLL files are platform specific.

Windows 2003:
To resolve the issue, please follow the instructions below:

1. Please backup the registry key -
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions

2. Remove this registry key along with all its sub-keys

3. Reboot the machine

Although, it is not an official recommendation from Microsoft, this key will get recreated after the machine is restarted.

Notes:
If you are running an older version of AhsayOBM / AhsayACB (Pre-5.2.4.0), you could consider patching the AhsayOBM / AhsayACB software to the latest patch release. The instruction can be found by Clicking Here.

2.10 Backup Interrupted by System Error Maximum retry reached

When performing a backup of any type, the following job status is received in the backup report:

Backup Interrupted by System Error "Maximum retry reached"

Upon further investigation, the following informative / warning message is received in the client log:

[YYYY-MM-DD hh:mm:ss][erro] Backup Interrupted by System Error "[Thread][BackupSet Dispatcher][BackupSet][BackupSetDispatcher.sendRequest] Maximum retry reached"

The message suggests that there is problem with the connection between the AhsayOBM client and the AhsayOBS server. Furthermore, the maximum number of attempts to re-establish the connection has been reached. Thus, the backup is then terminated by the system.

If the issue only occurs occasionally, you can safely ignore the error.

In the cases where the issue persists, please ensure that the connection to the AhsayOBS server can be established during the backup process.

2.11 Orphan checksum pair file. Deleting backup file

When performing a backup of any type, the following error message is received in the backup report:

Orphan checksum pair file. Deleting backup file -
ServerPath='User_Home\User\files\Backup_ID\Current\xxxx\xxxx\xxxx\xxxx*.chk'
BackupSet='Backup_Set(Backup_ID)' BackupJob='Current' ClientPath='Directory_Path\File'
RunByBackupJob='YYYY-MM-DD-hh-mm-ss'

The message suggests that the AhsayOBS server located a checksum file on server, but the corresponding data file cannot be found (or vice versa).

To resolve the issue, please rebuild the User Storage for the corresponding user in concern.

You can do so by logging into AhsayOBS management console, and then select [Manage User] -> [User Profile], you should see an option just under the user summary called [File Validation Option], clicking on this will display the options and a [Check] button. Enable the [Verify Checksum] option, and click on the [Check] button to start the single user rebuild.

Please allow the rebuild user storage job to run to its completion, and then perform a manual backup afterward.

If you are running an older version of AhsayOBS (Pre-5.2.4.0), please also consider patching the AhsayOBS server to the latest patch release. The instruction can be found by Clicking Here.

Notes:

When the single user rebuild is completed, the user statistic of the corresponding user will be displayed in the system log. The system log can be found under the AhsayOBS management console: [Manage Log] -> [System Log]

2.12 In-file delta file chain broken. Deleting backup file

When performing a file backup, the following error message is received in the backup report:

In-file delta file chain broken. Deleting backup file - ServerPath='User_Home\ Username\files\Backup_ID\Current\xxxx\xxxx\xxxx\xxxx*.del' BackupSet='Backup_Set(Backup_ID)' BackupJob='Current' ClientPath='Directory_Path\File' Type='I' RunByBackupJob='YYYY-MM-DD-hh-mm-ss'

The message suggests that there is a problem with the chain of delta file(s) on server.

To resolve the issue, please rebuild the User Storage for the corresponding user in concern.

You can do so by logging into AhsayOBS management console, and then select [Manage User] -> [User Profile], you should see an option just under the user summary called [File Validation Option], clicking on this will display the options and a [Check] button. Enable the [Verify Checksum] option, and click on the [Check] button to start the single user rebuild.

Please allow the rebuild user storage job to run to its completion, and then perform a manual backup afterward.

If you are running an older version of AhsayOBS (Pre-5.2.4.0), please also consider patching the AhsayOBS server to the latest patch release. The instruction can be found by Clicking Here.

Notes:
When the single user rebuild is completed, the user statistic of the corresponding user will be displayed in the system log. The system log can be found under the AhsayOBS management console: [Manage Log] -> [System Log]

2.13 [UserCacheManager.NoSuchUserExpt] User not found

The following informative messages are found in the AhsayOBS system log:

[GetUserProfileRqt]Throwable='[UserCacheManager.NoSuchUserExpt] User 'Username' not found.'

The message suggests that the AhsayOBM / AhsayACB user(s) has been removed from the AhsayOBS server. However, the AhsayOBM / AhsayACB scheduler service on the corresponding machine is still running.

As the scheduler service attempts to establish connection to the AhsayOBS server, a message would be displayed in the system log suggesting that the user cannot be found.

These are information messages that you can safely ignored.

In the cases where the messages are causing concern, you can un-install the AhsayOBM / AhsayACB software on the corresponding client machine to resolve the issue.

## 2.14 Skip backing up "\\Network_Path\Directory" (network drive is not accessible)

When performing a file backup on network drive, the following warning messages are received in the backup report:

"\\Network_Path\Directory" The specified username is invalid.
Skip backing up "\\Network_Path\Directory" (network drive is not accessible)

The message suggests that the login credentials entered in the "User Authentication for Windows" setting for the affected backup set does not have sufficient permission to access the network drive.

To resolve the issue, please ensure that the login credentials specified in the "User Authentication for Windows" setting does have sufficient right to access the network drive.

Example on AhsayOBM:
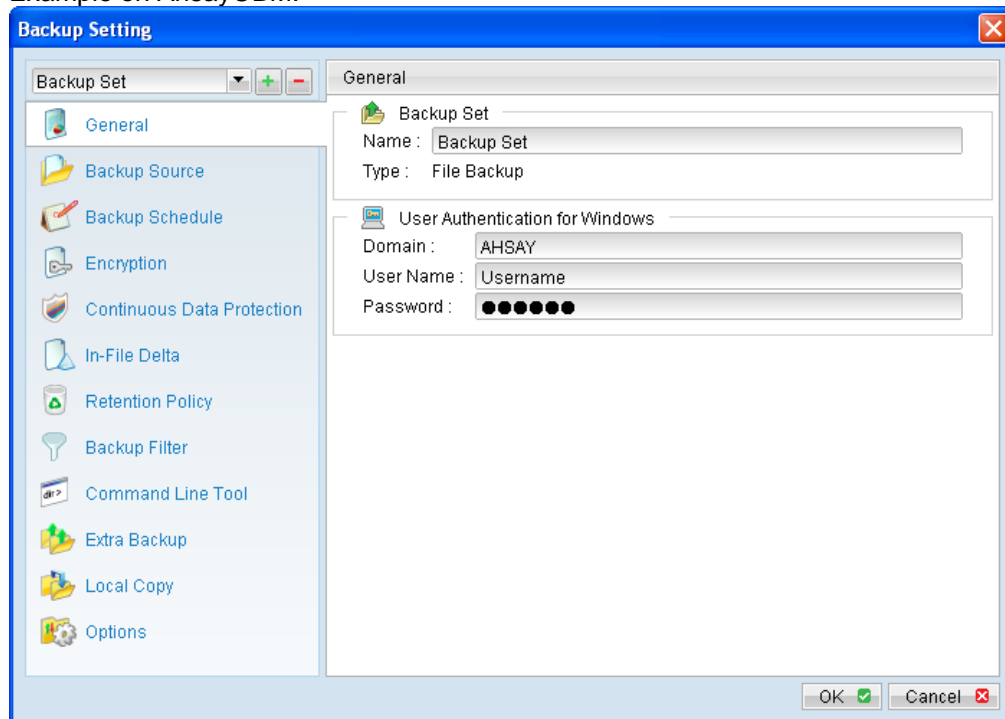
If the problem persist, please also verify if the "Log on" account of the AhsayOBM / AhsayACB scheduler service has sufficient permission right(s) to access the network drive. Alternatively, instead of "Local System", please try running the backup scheduler service with a Windows account that has sufficient permission right(s) to access the network drive. You can do so by following the instructions below:

1. Open [Control Panel] -> [Administrative Tools] -> [Services] -> [Online Backup Scheduler (Ahsay Online Backup Manager)] -> [Log on]
2. Select the [This Account] option
3. Enter the Login Credentials
4. Restart the [Online Backup Scheduler (Ahsay Online Backup Manager)] service

Notes:
For issue with AhsayACB, please edit the Login Credentials for the backup scheduler service [Online Backup Scheduler (Ahsay A-Click Backup)] instead.

2.15 'Connection timed out: connect'. Still Fail After Retry

When performing a backup of any type, the following error message is received in the backup report:

Unable to log to server. Error="[YYYY/MM/DD hh:mm][Http.doPost] Error='Connection
timed out: connect'. Still Fail After Retry!!!!"

The message suggests that there is problem with the connection between the AhsayOBM / AhsayACB
client and the AhsayOBS server.

If the issue only occurs occasionally, you can safely ignore the error. In most cases, AhsayOBM /
AhsayACB will attempt to re-establish connection to the AhsayOBS server.

In the cases where the issue persist, please ensure that the connection to the AhsayOBS server can be
established during the backup process.

2.16 Incomplete backup file deleted because the file was not updated within the last 48 hours

When performing a backup of any type, the following informative message is received in the backup report:

Incomplete backup file deleted because the file was not updated within the last 48 hours.. Deleting backup
file - ServerPath='\User_Home\File' BackupSet='Backup_Set(Backup_ID)' BackupJob='Current'
ClientPath='\Directory_Path\File' Type='F' RunByBackupJob='YYYY-MM-DD-hh-mm-ss

The message suggests that the upload of the corresponding file has not been completed, and there is no
update on the file within the next 48 hours. Thus, the incomplete file is removed from the AhsayOBS server.

Since the incomplete file has been removed from the AhsayOBS server, the file would be uploaded again
when the next backup job is performed. If the issue only occurs occasionally, you can safely ignore the error.

In the cases where the issue persist, please ensure that the connection to the AhsayOBS server can be
established during the backup process.

2.17 Path "Directory_Path\Directory" does not exist!

When performing a file backup, the following warning message is received in the backup report:

Path "Directory_Path\Directory" does not exist!

However, the directory path in concern has been removed from the backup source already.

The message suggests that the mentioned path is still being selected as part of the backup source. This
warning message can also be flagged if a backup filter is still being set to be applied on the mentioned
directory path.

To resolve the issue, please ensure that the corresponding directory path is removed from the backup
source of the affected backup set. Please also verify if there is any filter that may be applied to the directory
path in concern.

2.18 The device is not ready (Volume Shadow Copy issue)

When performing a file backup, the following error messages are received in the backup report:

[Error][New File] File="\Directory_Path\File" Error="The device is not ready. "

The message suggests that AhsayOBM / AhsayACB has problem reading the backup source media. Some possible causes of this issue could be hardware problem on the media in concern, Volume Shadow Copy issue, etc.

Windows XP / Vista:
To resolve the issue, please re-register the Volume Shadow Copy Service. To do so, you could utilize the "RegisterVSS.bat" script available in ${Install-Home}\bin. Please also reboot the machine afterward.

Notes:
Please safely ignore the error message(s) displayed during the re-registration, as some of the DLL files are platform specific.

Windows 2003:
To resolve the issue, please follow the instructions below:

1. Please backup the registry key -
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions

2. Remove this registry key along with all its sub-keys

3. Reboot the machine

Although, it is not an official recommendation from Microsoft, this key will get recreated after the machine is restarted.

2.19 "\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy_number" does not exist

When performing a file backup, the following warning message is received in the backup report:

Path "C:\Directory -> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy_number\Directory" does not exist!

This is a Microsoft Volume Shadow Copy issue.

Windows XP / Vista:
To resolve the issue, please re-register the Volume Shadow Copy Service. To do so, you could utilize the "RegisterVSS.bat" script available in ${Install-Home}\bin\ or ${Install-Home}\bin\. Please also reboot the machine afterward.

Notes:
Please safely ignore the error message(s) displayed during the re-registration, as some of the DLL files are platform specific.

Windows 2003:
To resolve the issue, please follow the instructions below:

1. Please backup the registry key -
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions

2. Remove this registry key along with all its sub-keys

3. Reboot the machine

Although, it is not an official recommendation from Microsoft, this key will get recreated after the machine is restarted.

2.20 VSS_E_UNEXPECTED_PROVIDER_ERROR (Volume Shadow Copy issue)

When performing a file backup, the following error message is received in the backup report:

[ERROR] VSS_E_UNEXPECTED_PROVIDER_ERROR

Notes:
Since a shadow copy cannot be created, the error above will usually result with the following error being flagged as well:

[Error][Updated File] File="C:\Directory_Path\File" Error="The process cannot access the file because it is being used by another process."

This is a Microsoft Volume Shadow Copy issue.

Windows XP / Vista:
To resolve the issue, please re-register the Volume Shadow Copy Service. To do so, you could utilize the "RegisterVSS.bat" script available in ${Install-Home}\bin. Please also reboot the machine afterward.

Notes:
Please safely ignore the error message(s) displayed during the re-registration, as some of the DLL files are platform specific.

Windows 2003:
To resolve the issue, please follow the instructions below:

1. Please backup the registry key -
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions

2. Remove this registry key along with all its sub-keys

3. Reboot the machine

Although, it is not an official recommendation from Microsoft, this key will get recreated after the machine is restarted.

2.21 [ERROR] VSS_E_PROVIDER_VETO

When performing a file backup, the following informative messages are received in the backup report:

[Shadow Copy] (1/10) Will retry in 60 Sec.
[Shadow Copy] (2/10) Will retry in 60 Sec.
...
[Shadow Copy] (10/10) Will retry in 60 Sec.
[ERROR] VSS_E_PROVIDER_VETO

Notes:
Since a shadow copy cannot be created, the error above will usually result with the following error being flagged as well:

[Error][Updated File] File="C:\Directory_Path\File" Error="The process cannot access the file because it is being used by another process."

The message suggests that the file(s) being backed up is on a FAT32 partition and either there is no NTFS partition on an internal drive or that NTFS partition has less than 100MB of free disk space.

The problem can also occur if the disk activity was high when the backup job is performed.

To resolve the issue, please correct the partition issues suggested above and perform the backup again.

Please also verify if there is other application(s) running on the corresponding machine, which may require a high amount of disk resources. Alternatively, you can perform the backup when disk usage is low.

2.22 [ERROR] VSS_E_WRITER_INFRASTRUCTURE

When performing a file backup, the following informative messages are received in the backup report:

[Shadow Copy] (1/10) Will retry in 60 Sec.
[Shadow Copy] (2/10) Will retry in 60 Sec.
...
[Shadow Copy] (10/10) Will retry in 60 Sec.
[ERROR] VSS_E_WRITER_INFRASTRUCTURE

Notes:
Since a shadow copy cannot be created, the error above will usually result with the following error being flagged as well:

[Error][Updated File] File="C:\Directory_Path\File" Error="The process cannot access the file because it is being used by another process."

This is a Microsoft Volume Shadow Copy issue.

Windows XP / Vista:
To resolve the issue, please re-register the Volume Shadow Copy Service. To do so, you could utilize the "RegisterVSS.bat" script available in ${Install-Home}\bin. Please also reboot the machine afterward.

Notes:
Please safely ignore the error message(s) displayed during the re-registration, as some of the DLL files are platform specific.

Windows 2003:
To resolve the issue, please follow the instructions below:

1. Please backup the registry key -
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions

2. Remove this registry key along with all its sub-keys

3. Reboot the machine

Although, it is not an official recommendation from Microsoft, this key will get recreated after the machine is restarted.

**2.23 File="\\Network_Drive\Directory_Path\File" Error="Access is denied."**

When performing a file backup, the following error messages are received in the backup report:

File="\\Network_Drive\Directory\File" Error="Access is denied."

The message suggests that the login credentials specified in the "User Authentication for Windows" setting of the file backup set does not have sufficient right to access the file or directory specified.

Please ensure that the login credentials specified in the "User Authentication for Windows" setting does have sufficient right to access the file or directory.

Example with AhsayOBM:
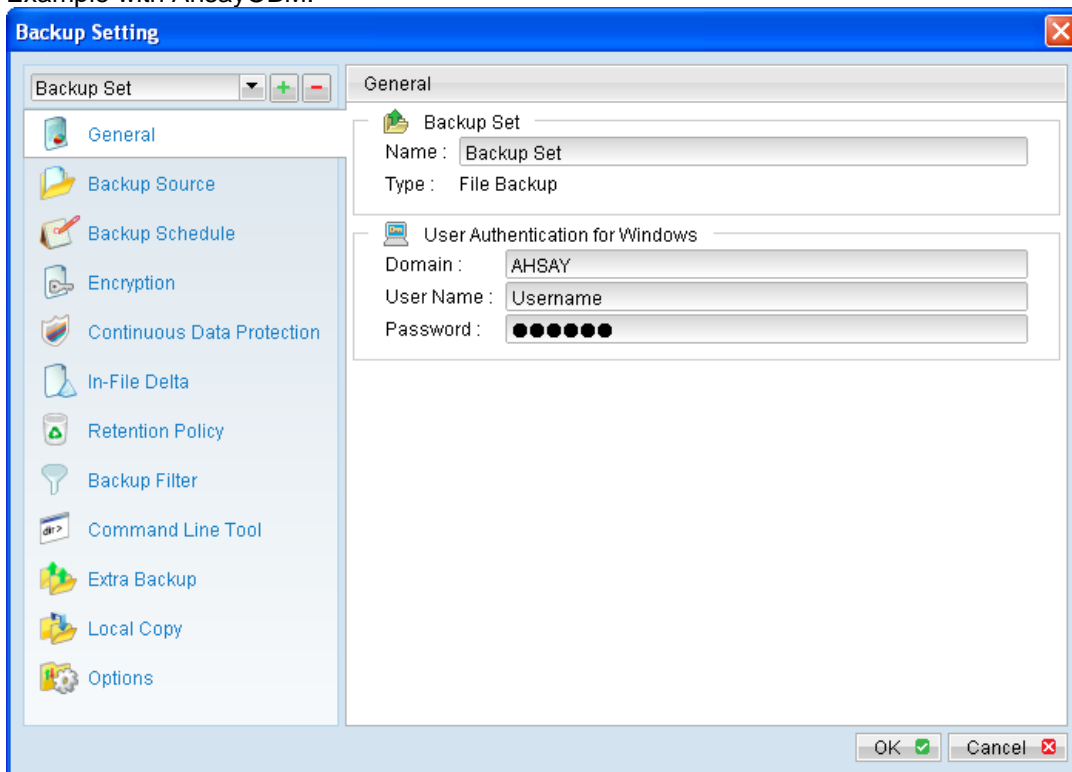
If the problem persist, please also verify if the "Log on" account of the AhsayOBM / AhsayACB scheduler service has sufficient permission right(s) to access the temporary directory.

Alternatively, instead of "Local System", please try running the AhsayOBM / AhsayACB scheduler service with a Windows account that has sufficient permission right(s) to access the temporary directory. You can do so by following the instructions below:

1. Open [Control Panel] -> [Administrative Tools] -> [Services] -> [Online Backup Scheduler (Ahsay Online Backup Manager / Ahsay A-Click Backup)] -> [Log on]
2. Select the [This Account] option
3. Enter the Login Credentials
4. Restart the [Online Backup Scheduler (Ahsay Online Backup Manager / Ahsay A-Click Backup)] service

2.24 A newer version of this software already exists on this volume

When installing AhsayOBM / AhsayACB on a Mac OS X machine, the following error message is shown:

> (!) You cannot install Ahsay Online Backup Manager on this volume. A newer version of this software already exists on this volume.
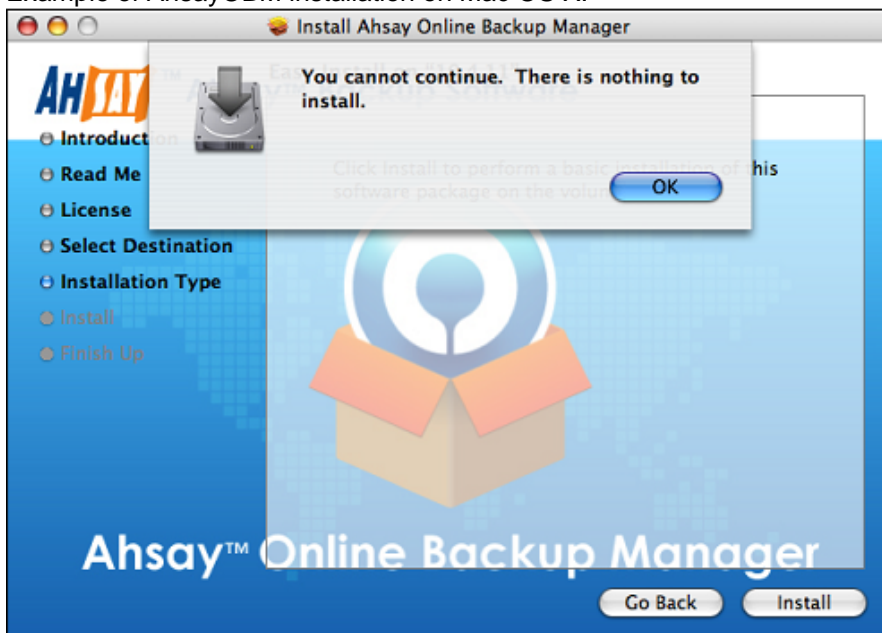
Example of AhsayOBM installation on Mac OS X:
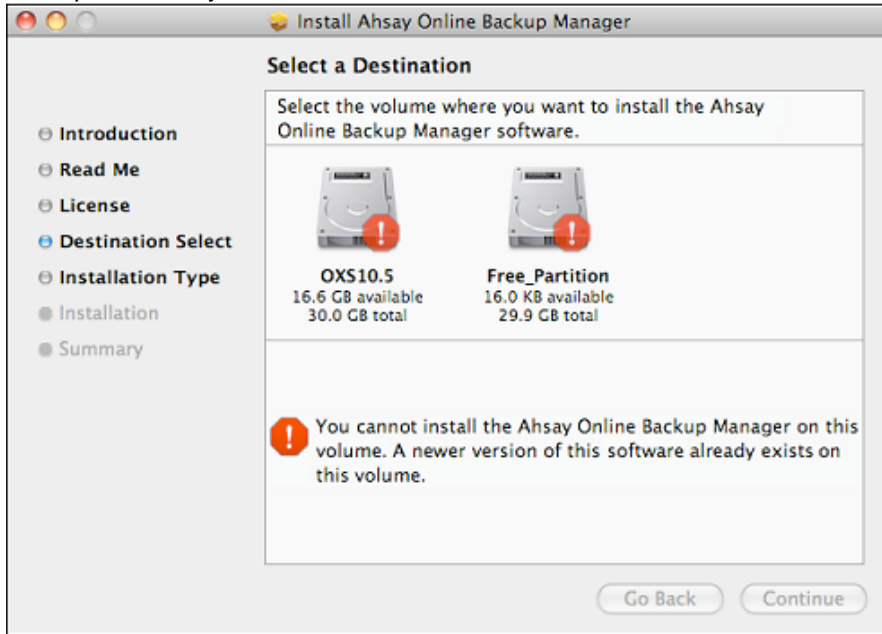
or

You cannot continue. There is nothing to install.

Example of AhsayOBM installation on Mac OS X:

The message suggests that there is configuration file(s) left over from the previous installation of AhsayOBM / AhsayACB.

To resolve the issue, please follow the instructions below:

1. Navigate to the directory /Library/Receipts:

Example:
>ls -la /Library/Receipts

2. Remove all Ahsay referenced package files, such as acb.pkg, obm.pkg or obc.pkg

3. Install the AhsayOBM / AhsayACB software afterward

2.25 Checksum of file \Directory_Path\File is incorrect. Deleting backup file

When performing a backup of any type, the following error message is received in the backup report:

Checksum of file \User_Home\Username\files\Backup_ID\Current\xxxx\xxxx\xxxx\xxxx\File is incorrect. Deleting backup file - ServerPath='\User_Home\User\files\Backup_ID\Current\xxxx\xxxx\xxxx\File' BackupSet='Backup_Set(Backup_ID)' BackupJob='Current' ClientPath='\Directory_Path\File' Type='C' RunByBackupJob='YYYY-MM-DD-hh-mm-ss'

The message suggests that the checksum value of the corresponding data file on the AhsayOBS server is not correct.

You can safely ignore the error, as the incorrect file has been removed from the AhsayOBS server, the file would be uploaded again when the current backup job is performed.

Please also verify if there are hardware or I/O issues with the corresponding User Home partition.

Windows:
For AhsayOBS running on Windows, please verify under [Control Panel] -> [Administrative Tools] -> [Event Viewer] if an error could be found. If a disk error is found, please perform a checkdisk on the corresponding partition by entering the command "chkdsk /f" in command prompt.

Linux/Unix:
For AhsayOBS running on Linux/Unix, depending on the distribution, you could try entering the command "cat /var/log/messages" and verify if an error could be found. If a disk error is found, please perform a checkdisk on the corresponding partition by enter the command "/sbin/fsck" and "/sbin/e2fsck" (with the partition un-mount).

2.26 No checksum file found. File "Directory_Path\File" is being backed up in its entirety …

When performing a backup of any type, the following informative message is received in the backup report:

No checksum file found. File "Directory_Path\File" is being backed up in its entirety along with its checksum file

The message suggests that the checksum file of the corresponding data file on the AhsayOBS server is missing or corrupted.

You can safely ignore the message, as the checksum file along with the data file would be uploaded again when the current backup job is performed.

Please also verify if there are hardware or I/O issues with the corresponding User Home partition.

Windows:
For AhsayOBS running on Windows, please verify under [Control Panel] -> [Administrative Tools] -> [Event Viewer] if an error could be found. If a disk error is found, please perform a checkdisk on the corresponding partition by entering the command "chkdsk /f" in command prompt.

Linux/Unix:
For AhsayOBS running on Linux/Unix, depending on the distribution, you could try entering the command "cat /var/log/messages" and verify if an error could be found. If a disk error is found, please perform a checkdisk on the corresponding partition by enter the command "/sbin/fsck" and "/sbin/e2fsck" (with the partition un-mount).

2.27 [StartBackupRqt] Error='null'. Client agent will retry shortly

When performing a backup of any type, the following error message is received in the backup report:

[StartBackupRqt] IP='User-IP-Address' User='Username' BackupSet='Backup Set (BackupID)' BackupJob='YYYY-MM-DD-hh-mm-ss' StartTime='YYYY-MM-DD hh:mm:ss' CurrentTime='YYYY-MM-DD hh:mm:ss' Error='null'. Client agent will retry shortly.

The message suggests that the request for a backup set's file list from the AhsayOBS server has timed out.

When a backup job is initiated, the AhsayOBM client would requests for a backup set's file list from the AhsayOBS server. As the request is made, AhsayOBS will generate the file list and compress this information to "block" file(s), where the block(s) are then sent to the AhsayOBM client (as each block is generated).

During the generation of the file list , if the time taken exceeded the timeout period for AhsayOBM, the retry message is flagged. AhsayOBM would also submit this retry null error to AhsayOBS.

Notes:
Some partners had suggested that this error is occurring more frequently after the upgrade to version 5.5.3.x.

The reason why you may be seeing this issue more often after an upgrade to version 5.5.3.x, is because of the index migration process involved. With the index migration performed when a backup is initiated, the time it takes for AhsayOBS to generate the file list "block" may be longer, hence, resulting in a larger number of "client retry" problem.

In most cases, even with this error, AhsayOBM will re-attempt the request and the backup job would eventually be performed to completion.

For all backup users with similar issue, please verify on the backup report of the corresponding job(s) to confirm if the backup job was eventually completed with this error:

For cases where the backup job was eventually completed, our software development team is aware of the concern generated by the message. Since the backup job was actually performed, such issue with retry mechanism would be changed to an informative message instead of an error in the next hot-fix release of AhsayOBS.

For cases where the backup job was not performed after the retry message, the cause may be different than the one we have outlined above. For these cases, please submit a Support Ticket for us to further troubleshoot on the case.

2.28 File exists already. It should not be overwritten

When performing a backup of any type, the following error message is received in the backup report:

User="Username" sBackupSet=BackupSet-ID(BackupSet) sClientPath="\Directory\File' '(YYYY-MM-DD hh:mm:ss) ServerPath="\User-Home\files\BackupSet\Current\xxxx\xxxx\xxxx\xxxx\File"(YYYY-MM-DD hh:mm:ss FileBlockSeq=1) exists already. It should not be overwritten. Please run [Manage User] -> [User Profile] -> [File Validation Option] -> [Check] to correct this problem.

This is a known issue with AhsayOBM version 5.5.5.0 or above.

To resolve the issue, please patch the AhsayOBM software to the latest patch release.

The instruction can be found by Clicking Here.