Getting Started with Zmanda Cloud Backup (ZCB)

Zmanda Cloud Backup (previously called Zmanda Internet Backup) is a secure and convenient way to back up Windows workstations and servers to Local Folder or Cloud storage (Amazon S3). Amazon S3 certificate is required to perform backup and recovery to the cloud. This certificate can be purchased from Zmanda Network or by using **Cloud > Purchase Subscription** from the ZCB user interface.

With Zmanda Cloud Backup, you can select any of the following as backup objects:

- Windows NTFS files and folders
- Microsoft SQL Server 2000, 2005 and 2008
- Microsoft Exchange Server 2003 and 2007
- Microsoft Share Point Server 2007 and WSS 3.0
- Oracle Server 11g running on Windows
- MySQL server 5.x
- Windows System State (registry, certificate server and active directory information)

SQL Server, Exchange Server, SharePoint server and Oracle Server configurations are discovered. No additional configuration is necessary. Zmanda Cloud Backup has options to use native Windows compression and digital certificate based encryption for backup data.

System Requirements

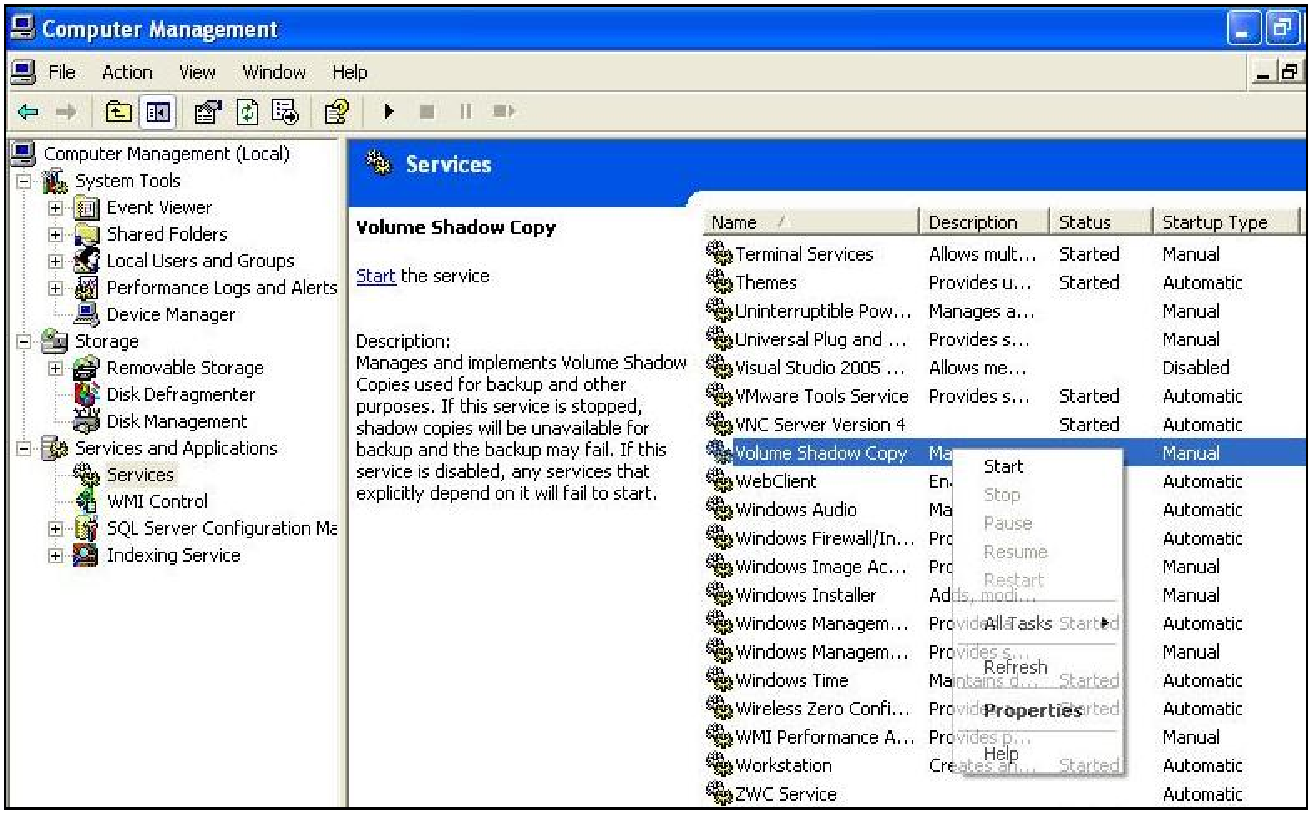
If you are having problems running ZCB, check that your system meets these requirements:

- Check that the ZCB server is connected to the internet, and that you have a valid S3 subscription. The ZCB **Tools** menu includes a **Check S3 connection** option for this purpose.

- Java Runtime Environment (JRE) 6 Update 16 or higher.

- The Volume Shadow Copy Service must be enabled. Although the Volume Shadow Service is enabled by by default, it may have been turned off after Windows installation. To ensure that it is running:

  1. Right-click the **My Computer** icon and choose **Manage** from the pop up menu.
  2. Expand the Services and Applications tree and locate the **Volume Shadow Copy** Service.



Volume Shadow Copy

Start the service

Description:
Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type
Terminal Services	Allows mult...	Started	Manual
Themes	Provides u...	Started	Automatic
Uninterruptible Pow...	Manages a...		Manual
Universal Plug and ...	Provides s...		Manual
Visual Studio 2005 ...	Allows me...		Disabled
VMware Tools Service	Provides s...	Started	Automatic
VNC Server Version 4		Started	Automatic
Volume Shadow Copy	Ma		Manual
WebClient	En		Automatic
Windows Audio	Ma		Automatic
Windows Firewall/In...	Pro		Automatic
Windows Image Ac...	Pro		Manual
Windows Installer	Adds, modi...		Manual
Windows Managem...	Provid	Started	Automatic
Windows Managem...	Provides s...		Manual
Windows Time	Maintains d...	Started	Automatic
Wireless Zero Confi...	Provid	Started	Automatic
WMI Performance A...	Provides p...		Manual
Workstation	Creates an...	Started	Automatic
ZWC Service			Automatic

1. If it is not started, do so.
2. If necessary, change the General Properties to make the Startup Type **Automatic** rather than **Manual**.

- The Remote Registry Service must be enabled before installation.

- Zmanda Cloud Backup must be installed and all ZCB operations must be performed as an user that has Administrator privileges.

- Zmanda Cloud Backup stores the backup catalog in the Installation folder and not in Local Backup Folder. The backup index is very important for restoration of backup images. Administrators should ensure sufficient disk space is available in the Installation folder for backup catalog. The amount of space required depends on number of backup sets, backup images and number of files/objects in each backup image.

- Zmanda Cloud Backup requires access the following TCP ports: Port 10080 & 10081, which are default ports used by ZCB for backup and restore. If the default ports are in use, alternate ports that are available at the time of installation are used. The ports used by the product can be modified using **Tools > Advanced Options** in the ZCB user interface.

Installation

The Zmanda Cloud Backup product uses InstallShield installer. Run **setup.exe** from the zip archive file to run the installer. The installer will check for system requirements such as Java JRE before installation.

If you are planning to install ZCB on multiple machines, you should record the user input for playback. Using the user input recorded file, you can install ZCB using command line on multiple machines in an unattended manner.

To record user input, run

setup.exe /r /f1<*recording file*>

The recording file will contain all user input for playback.

ZCB installer can read the user input recorded file from the same directory. Alternate location for user input can be provided using /f1 option. The installation log file will be created in same directory (default: Setup.log). Alternate location for the log can be provided using /f2 option. An example command for replaying user input from C:\Temp\Setup.iss file.

setup.exe /s /f1"C:\Temp\Setup.iss"

The command will complete before the installation or uninstallation process is completed. Use /WAIT flag if you want the setup.exe command to wait for the process to be completed. For example: Run the following installation command that will wait till process is completed in Windows command shell

start /WAIT setup.exe /w /s /f1"C:\tmp\Setup.iss"

The Zmanda Network provides default install.iss and uninstall.iss that can be used of unattended installation and uninstallation. This setup files assumes

1. ZCB will be installed in **C:\Program Files\Zmanda\Zmanda Cloud Backup** folder. The **amandabackup** password will be **password**

2. ZCB uninstallation will not preserve configuration data

About Backup Sets

All activities in ZCB are applied to backup sets. A backup set defines the parameters (the what, where, and when) for backing up a group of directories or an application such as Exchange. Each backup set can only be of a single type. For example, you cannot back up an Exchange server and and Windows System state in the same backup set.

Backup sets are listed along the left edge of the ZCB display. You can create, edit, activate, deactivate backup sets, and initiate an immediate backup by right-clicking a set and choosing from the pop-up menu. Backup set names are limited to 32 alphanumeric characters. A backup set must be activated (which is the default state) for the backups it defines to actually be performed as scheduled.

When a backup is performed, ZCB creates a local backup archive, which consists of the data being backed up (compressed in a .ZIP file), the backup index, and metadata associated with the backup.

All common tasks that are performed for a backup set are organized in **Tasks** drop down menu.

All operations that are common to all backup sets are organized in the **File**, **Cloud**, **Tools**, **Help** menu. The **File** menu has backup set meta operations (create, delete, validate and deactivation).

Configuring Backups

Zmanda Cloud Backup makes it easy to select **What**, **Where**, and **When** to back up by clicking the tabs beneath the menu bar and setting options as desired. To display these tabs, click on the desired backup set along the left side of the display, and make sure the **Tasks** drop-down menu is set to **Backup**.

Backup Set Panel

The backup set left panel in the UI shows all the configured backup sets and status of last job performed on the backup set (backup/restore/download/upload job). Hovering the mouse over the backup set provides details of the backup set job. Please note that there can be still older jobs being running for the backup sets. Please use the **Monitor** page for the backup set to get complete job information.

The right click menu in the pane allows users to perform backup set operations – creation, deletion, deactivation and validation as well as start jobs on the backup set.

Backup set configurations are automatically validated when configurations are saved as well as before any backup run is performed. Validation helps in catching configuration errors that could translate into backup or upload failures.

Deactivation of backup set prevents stops all scheduled backup/upload tasks for the backup set.

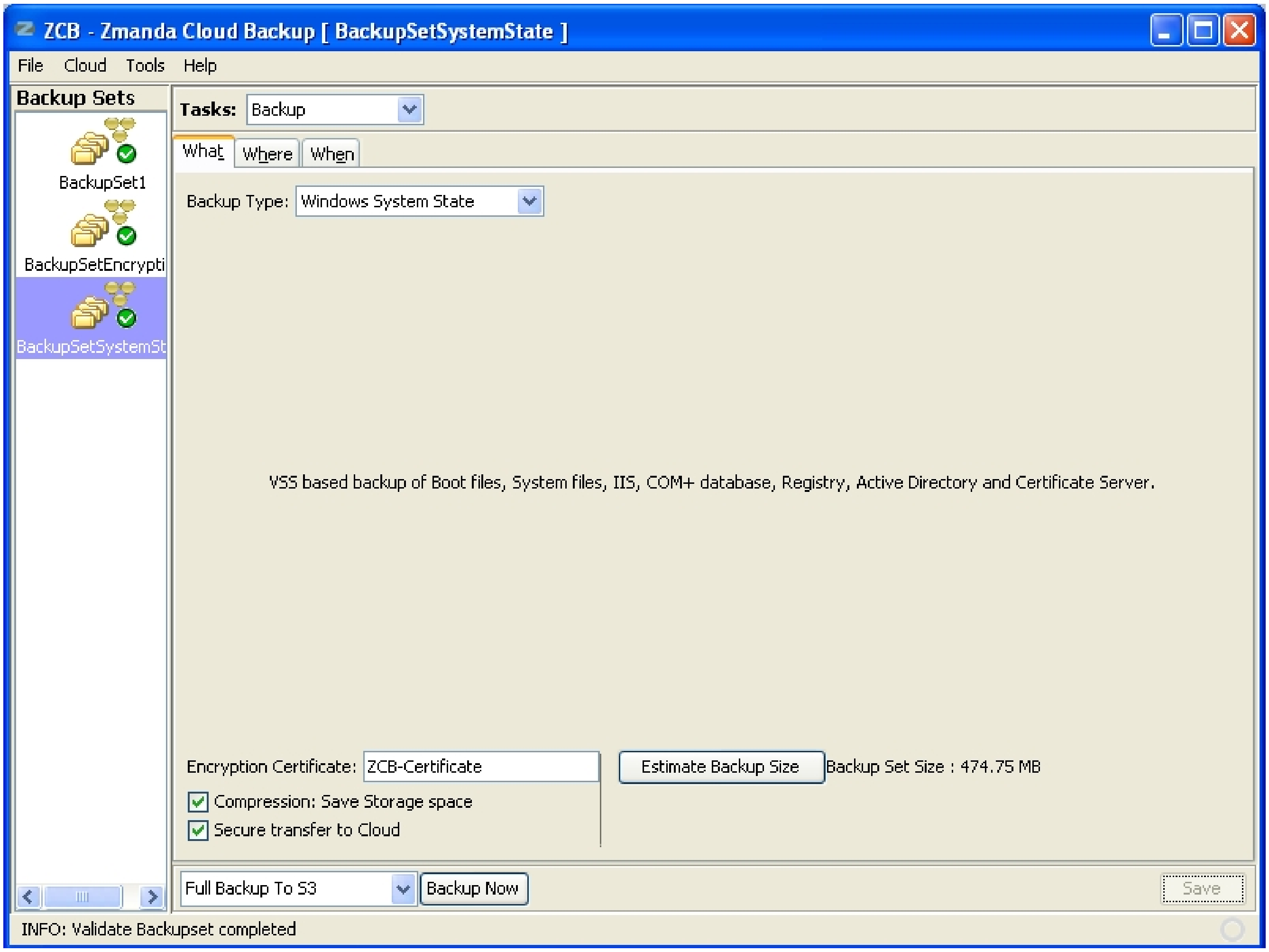
Choosing What to Back Up (Backup What tab)

The Backup **What** tab lets you select a **Backup Type** (such as **Windows File System**, **Windows system state**, and a number of common applications such as **Exchange**).

When backing up a NTFS file system, ZCB lets you select directories and files from a browser tree. You can specify the list of files to be excluded in case of Windows filesystem backup. Windows filesystems support wild cards in the exclude specification. Wild cards "*" (match one or more character) and "?" (match exactly one character) are supported. The pathname in exclude specification must be absolute path. For example: User is backing up **C:\Data** directory. User wishes to exclude files under a sub-folder **exclude** and files with ***.jpg** extension. The exclude specification should be **"C:\Data\exclude" "*.jpg"**

Users can also choose backup compression (**Compression: Save storage space** check box) to save the network bandwidth and backup storage space, backup encryption and secure transfer to Cloud using SSL. Users are recommended to use Compression and Secure transfer to Cloud for all backup sets. If the data being backed up is public such as public web sites, upload performance can be improved by not using secure transfer to cloud (internal testing has shown an improvement for 15-20% and actual performance improvement depends on lot of external factors).

Encryption is performed using digital certificates installed for the **amandabackup** user. See **Backup encryption** section for information how to add digital certificates for backup encryption. Digital certificates can be obtained from a CA (Certificate Authority) or self-signed. The digital certificate name must be specified in the Encryption text box field. The certificate name is case sensitive. In the screen image below, *ZCB-Certificate* has been specified. If no certificate is specified, data encryption is not performed. If the certificate is lost, the encrypted data cannot be recovered. It is very important to track and safeguard the encryption certificate.



Tasks: Backup

Backup Type: Windows System State

VSS based backup of Boot files, System files, IIS, COM+ database, Registry, Active Directory and Certificate Server.

Encryption Certificate: ZCB-Certificate

Backup Set Size : 474.75 MB

☑ Compression: Save Storage space

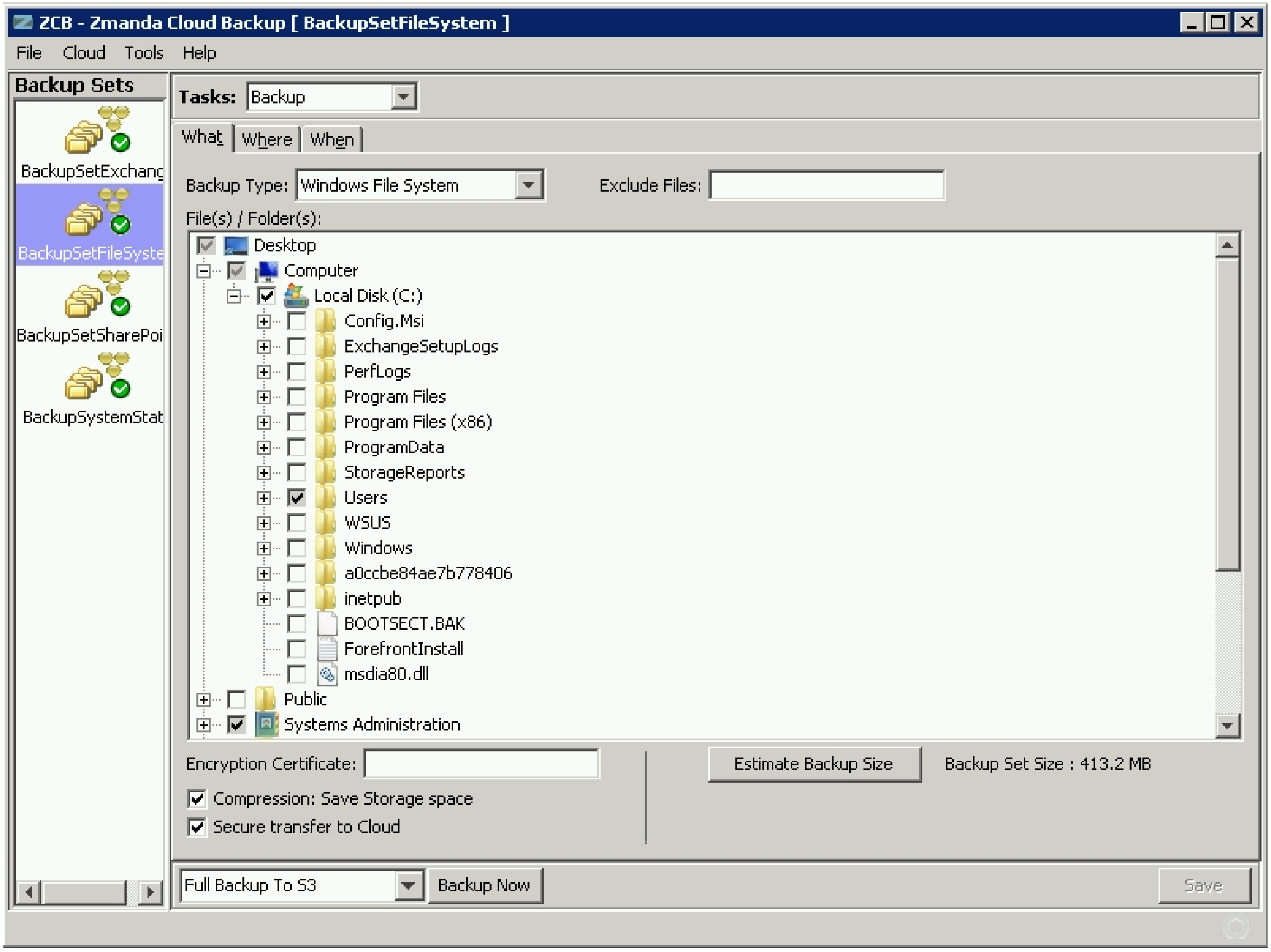
☑ Secure transfer to Cloud

Full Backup To S3

INFO: Validate Backupset completed

Backup data is encrypted and compressed before the backup data goes to the Backup Folder (local disk backup).

Backup What changes are validated before being saved. Validation checks for configuration errors and Volume Shadow Services (VSS) status.



ZCB - Zmanda Cloud Backup [BackupSetFileSystem]

Tasks: Backup

Backup Type: Windows File System

Exclude Files:

File(s) / Folder(s):

- ☑ Desktop
  - ☑ Computer
    - ☑ Local Disk (C:)
      - □ Config.Msi
      - □ ExchangeSetupLogs
      - □ PerfLogs
      - □ Program Files
      - □ Program Files (x86)
      - □ ProgramData
      - □ StorageReports
      - ☑ Users
      - □ WSUS
      - □ Windows
      - □ a0ccbe84ae7b778406
      - □ inetpub
      - □ BOOTSECT.BAK
      - □ ForefrontInstall
      - □ msdia80.dll
  - □ Public
  - ☑ Systems Administration

Encryption Certificate:

☑ Compression: Save Storage space

☑ Secure transfer to Cloud

Backup Set Size : 413.2 MB

Full Backup To S3

The list of patterns in the exclude specification for Windows file systems should be separated by space character.

Choosing an application from Backup Type drop down box adds all instances of the application running on the local server to the backup set. This implies:

Microsoft SQL server

VSS based backup of all the mounted databases and their log files.

Requirements:

- The Volume Shadow Copy Service must be enabled. This means that its startup type must be either automatic or manual.
- ZCB will only back up MS SQL databases that are in Mounted state.
- ZCB will only perform full backup of MS SQL databases.
- Microsoft recommends that MSSQL and System State back ups should not be run simultaneously.
- ZCB only backs up the MS SQL databases. It does not back up other MS SQL files such as program installation files, etc. To protect an MS SQL server from a disaster, make sure that you create a separate disk list entry to back up the other crucial MS SQL files.
- ZCB does not support component-based backup. It backs up all the mounted databases in the MS SQL server. Because it is not component-based, only databases with the Simple Recovery model are supported.
- ZCB does not use VSS for restores. Because ZCB does not support component-based backup,

post-restore Roll Forward is not supported.

Microsoft Exchange Server

VSS based backup of Store database files (.edb & .stm), transaction logs and checkpoint file for all the Mounted Storage Groups.

Requirements :

- The Volume Shadow Copy Service must be Enabled. Although the Volume Shadow Service is enabled by default, it may have been turned off after Windows installation. To ensure that it is running:
  - Right-click the My Computer icon and choose Manage from the popup menu.
  - Expand the Services and Applications tree and locate the Volume Shadow Copy Service.
  - If it is not started, do so. If necessary, change the General Properties to make the Startup Type Automatic
    rather than Manual.
- Run the command *vssadmin list writers* at the Windows command prompt and check that the state of the Exchange Writer is stable. If not (or if there are any VSS errors), restart the Volume Shadow Copy Service.
- In case of Windows 2003 Small Business Server edition, the Exchange Writer is disabled by default. Please follow the instructions this MS knowledgebase article to enable the Exchange Writer: http://support.microsoft.com/kb/838183
- Make sure that the Exchange Storage Groups are in Mounted state.
- Exchange circular logging must be disabled. If circular logging is enabled, the Exchange server client will only retain the last 5 transaction logs, which may not be sufficient to restore to the most recent backup.

Microsoft SharePoint Server

ZCB backs up and restores MS SharePoint (MOSS 2007 and WSS 3.0) at database level. ZCB backs up SharePoint data that is stored in the SQL database, such as

- Configuration and Admin databases
- Content and configuration data for Web Applications,
- Any third-party databases that are registered with SharePoint 2007
- Shared services databases in SharePoint 2007
- Office Search & Help Search index files

ZCB performs full backups of databases and rest of the SharePoint data incrementally backed up based on the modification time. The ZCB does not support transaction log based backup.
Since ZCB supports VSS based backup, SharePoint backup of individual objects such as Site collection, Web site, List/Document library, Document library folder, Document library file, List item, Version is not supported. Therefore files such as the SharePoint installation directory, IIS metabase information, Website application pool directory, etc require separate backup set configuration for backup.
ZCB currently supports only single server farm (standalone) configuration. In other words, the front-end server and the database server must reside on the same machine.

Requirements:

- Windows SharePoint Services VSS Writer service must be enabled and running. To enable and run the SharePoint writer follow the steps described in http://msdn.microsoft.com/en-us/library/bb447591.aspx.

- Windows SharePoint Services VSS Writer service must run under the **admin app pool** account, which is the **Network Service** account in a basic installation of Windows SharePoint Services.

Oracle on Windows

Archive Log Mode (ARCHIVELOGMODE) : VSS based backup of Open database, which includes online tablespaces, archive logs, snapshot control file and SPfile.
No Archive Log Mode (NOARCHIVELOGMODE) : VSS based backup of Mounted database, which includes, database files, snapshot control file and Spfile.

Requirements:

1. The ZCB supports backup and recovery of Windows Oracle 11i.

2. The Volume Shadow Copy Service must be enabled. Although the Volume Shadow Service is enabled by default, it may have been turned off after Windows installation. To ensure that it is running:

   - Right-click the **My Computer** icon and choose **Manage** from the popup menu.
   - Expand the Services and Applications tree and locate the **Volume Shadow Copy** Service.
   - Please start **Volume Shadow Copy** service.
   - Also, change the General Properties to make the Startup Type **Automatic** rather than **Manual**.

3. For backup in NOARCHIVELOGMODE, databases must be **Mounted** and in read-only state. The database cannot be open in NOARCHIVELOG mode, or the backup will fail. For backup in ARCHIVELOG mode, the database may be open and mounted. To determine the state of the database being backed up, enter **ARCHIVE LOG LIST** at the **sql** prompt, and look for the following output line:

   Database log mode No Archive mode or

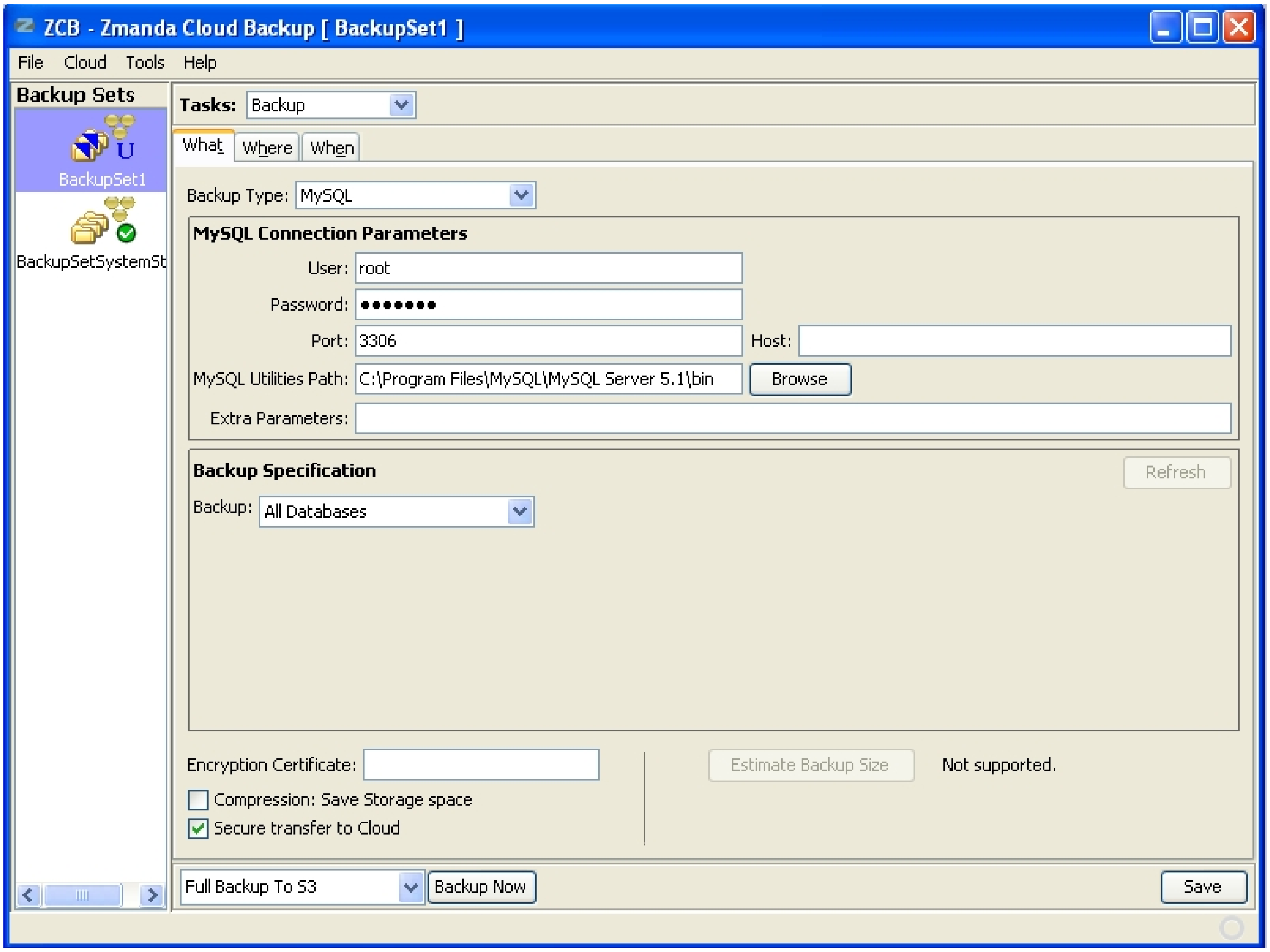
   Database log mode Archive mode

Windows System State

VSS based backup of Boot files, System files, IIS, COM+ database, Registry, Active Directory and Certificate Server.

MySQL server

Logical backup of MySQL databases and/or tables running on the ZCB machine or remote Linux server.



Tasks: Backup

Backup Type: MySQL

MySQL Connection Parameters

User: root

Password: •••••••

Port: 3306

Host:

MySQL Utilities Path: C:\Program Files\MySQL\MySQL Server 5.1\bin

Extra Parameters:

Backup Specification

Backup: All Databases

Encryption Certificate:

Not supported.

☐ Compression: Save Storage space

☑ Secure transfer to Cloud

Full Backup To S3

Each backup set can perform full backup of a MySQL server. In Backup What page, user can specify MySQL server information (IP address – **Host** and port number of the server – **Port**) and MySQL user information (user and password for the user that can perform the backup). The MySQL server can be running on the ZCB machine or remote MySQL server.

The MySQL user (**User**) should have sufficient privileges to perform logical backup from the ZCB machine. The minimal set of privileges required are

backup

LOCK TABLES, SELECT, FILE, RELOAD, SUPER, UPDATE, TRIGGER, SHOW VIEW

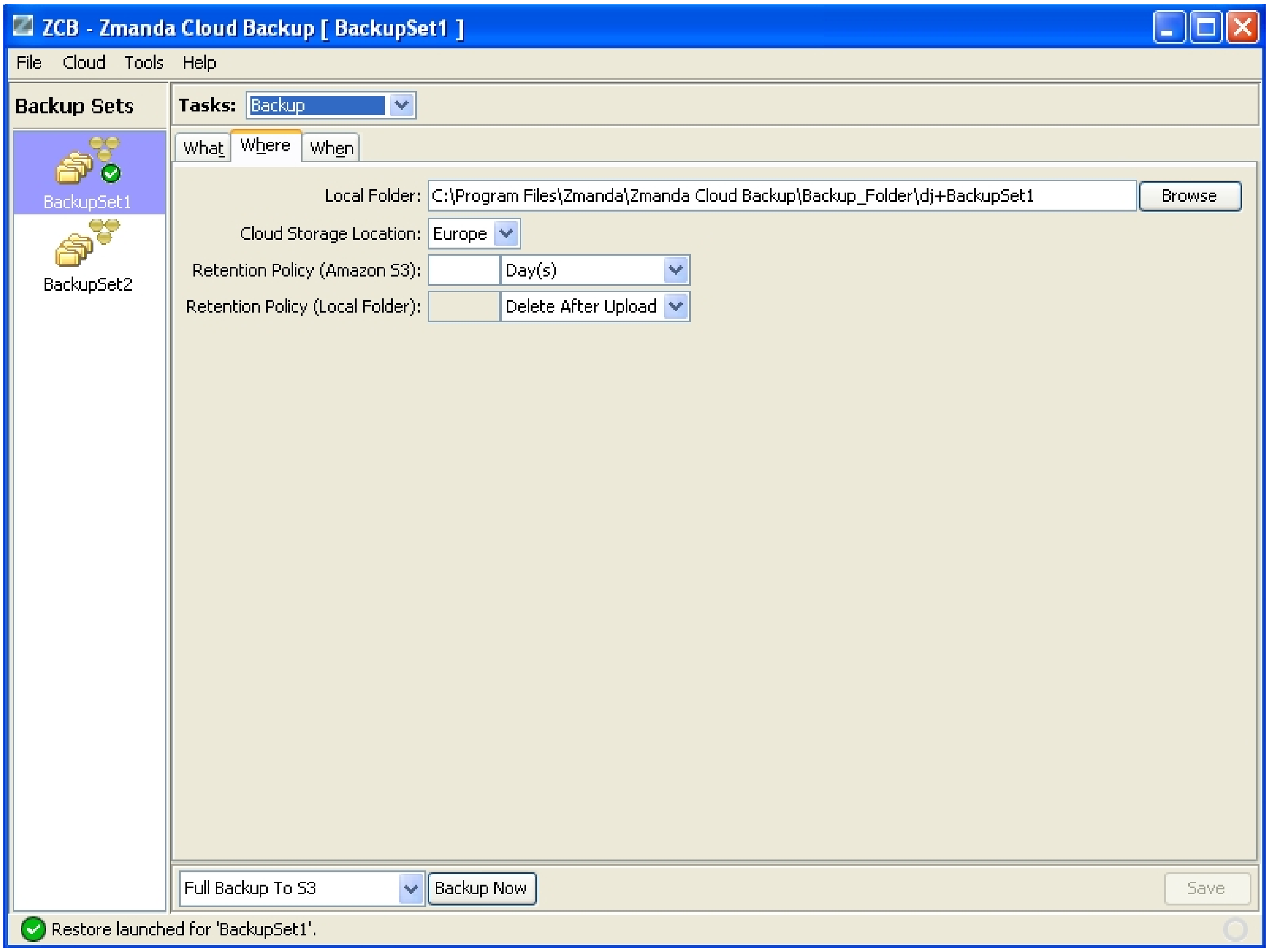
restoration

CREATE, DROP, INDEX, SHUTDOWN, INSERT, ALTER, UPDATE, TRIGGER, SUPER, REPLICATION CLIENT, CREATE VIEW

MySQL client utilities (**mysqldump** and **mysql**) must be installed on the ZCB machine and the MySQL client version must be compatible with MySQL server. The location of MySQL client utilities must be specified as **MySQL Utilities Path**. **Extra Parameters** can be used to specifying additional options to the MySQL backup program, **mysqldump**.

Users can perform backup of all databases on the server or selected databases or selected tables in a given database. Use **Refresh** button to update the list of databases and tables in the **Backup Specification** pane.

Choosing Where to Retain Local Backups (Backup Where tab)



Tasks: Backup

Local Folder: C:\Program Files\Zmanda\Zmanda Cloud Backup\Backup_Folder\dj+BackupSet1

Cloud Storage Location: Europe

Retention Policy (Amazon S3): Day(s)

Retention Policy (Local Folder): Delete After Upload

Full Backup To S3

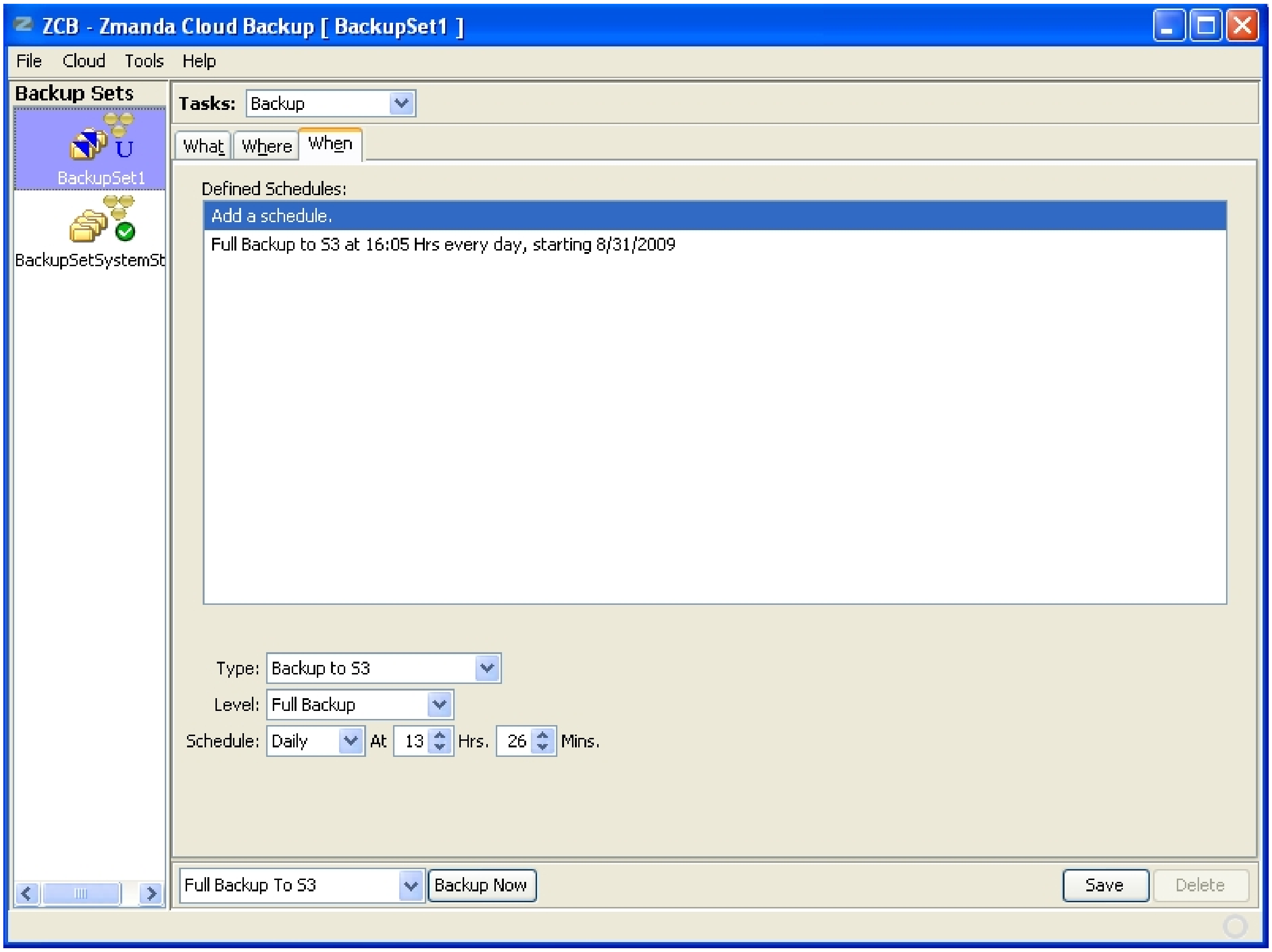
Restore launched for 'BackupSet1'.

ZCB lets you choose a local folder to store backup data, and how long to retain backups, both locally and on S3 storage. Choose an appropriate retention time, and make sure that the local folder you select (which will be used a staging area for the upload to remote storage) has enough available space. Specifying a **Retention Policy** of zero causes ZCB to retain the backups forever.

Please note the retention policy on the Amazon S3 is implemented as **Purge_ZIB_Backups** task scheduled on the Windows machine. This task is performed at midnight every day. This task should not removed from the Windows task scheduler. If the machine is not running at the time, backup images on the local folder as well as the cloud are not removed if retention policy has expired.

Scheduling a backup (Backup When tab)

ZCB allows you to schedule local backup and remote upload as a single operation or as separate operations, depending on the backup type you select. For example, **Backup to S3** backup type copies the data to the local directory specified on the **Backup Where** tab and then immediately uploads the data to S3. Alternatively, **Backup to Disk** and **Upload to S3** backup types perform these same actions separately, which allows you to schedule the upload when Internet traffic is light. You can specify a full or incremental backup regardless of type. Backup operations are scheduled as the Windows **System** user.



Tasks: Backup

Defined Schedules:

Add a schedule.

Full Backup to S3 at 16:05 Hrs every day, starting 8/31/2009

Type: Backup to S3

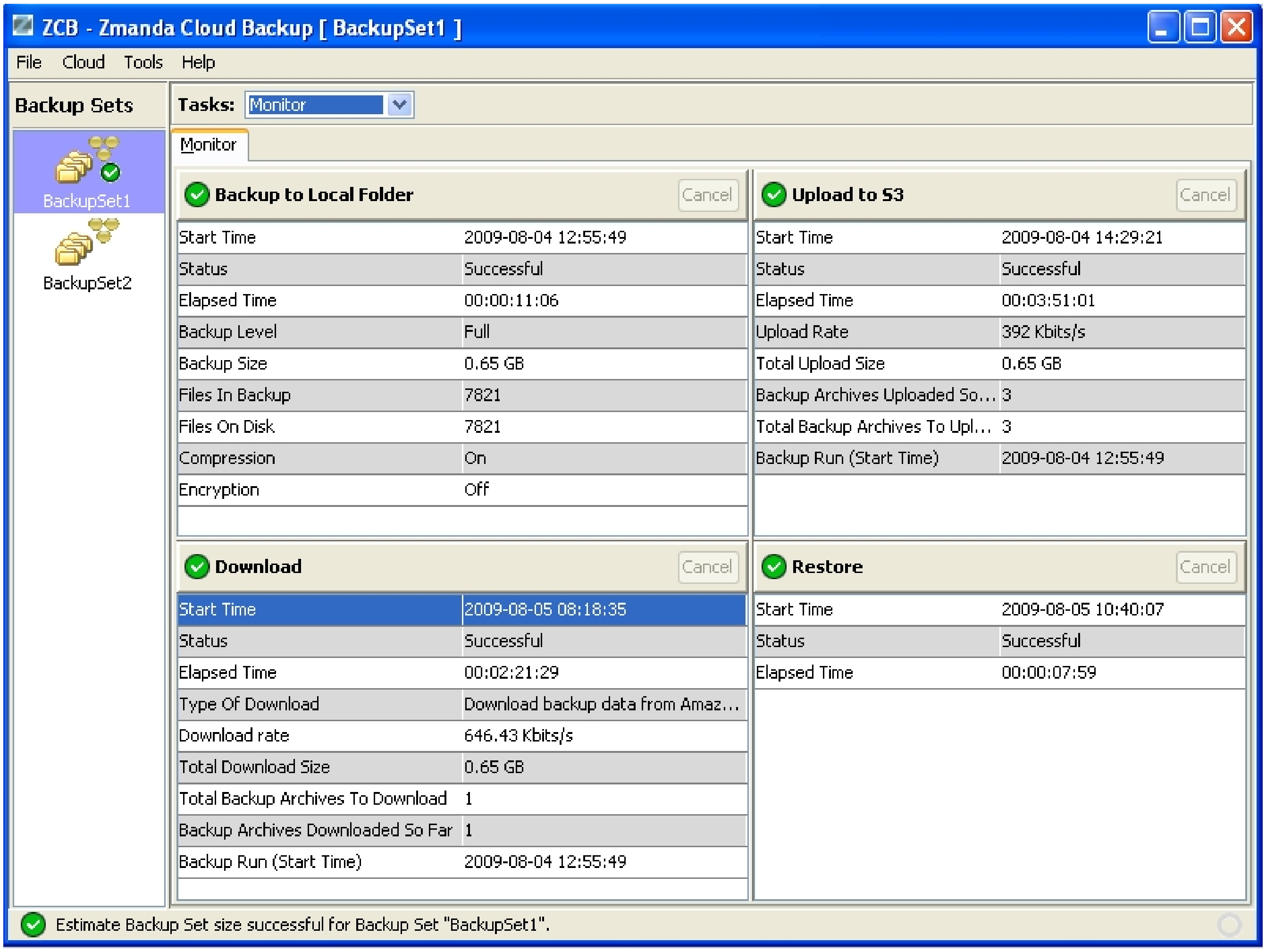
Level: Full Backup

Schedule: Daily At 13 Hrs. 26 Mins.

Full and Incremental backups to the Amazon S3 and Local Folder should can be immediately started using the drop down box in the **Backup When** and **Backup What** page. The backup set configuration is validated before the job is started.

Backup Administration (Monitoring and Reports)

Choose **Monitor** from the drop down menu in the upper right to display status of backups, restores, uploads and downloads in progress. Note that you can cancel any operation with the buttons provided in the upper right corner of each pane.



Tasks: Monitor

Backup to Local Folder

Start Time	2009-08-04 12:55:49
Status	Successful
Elapsed Time	00:00:11:06
Backup Level	Full
Backup Size	0.65 GB
Files In Backup	7821
Files On Disk	7821
Compression	On
Encryption	Off

Upload to S3

Start Time	2009-08-04 14:29:21
Status	Successful
Elapsed Time	00:03:51:01
Upload Rate	392 Kbits/s
Total Upload Size	0.65 GB
Backup Archives Uploaded So...	3
Total Backup Archives To Upl...	3
Backup Run (Start Time)	2009-08-04 12:55:49

Download

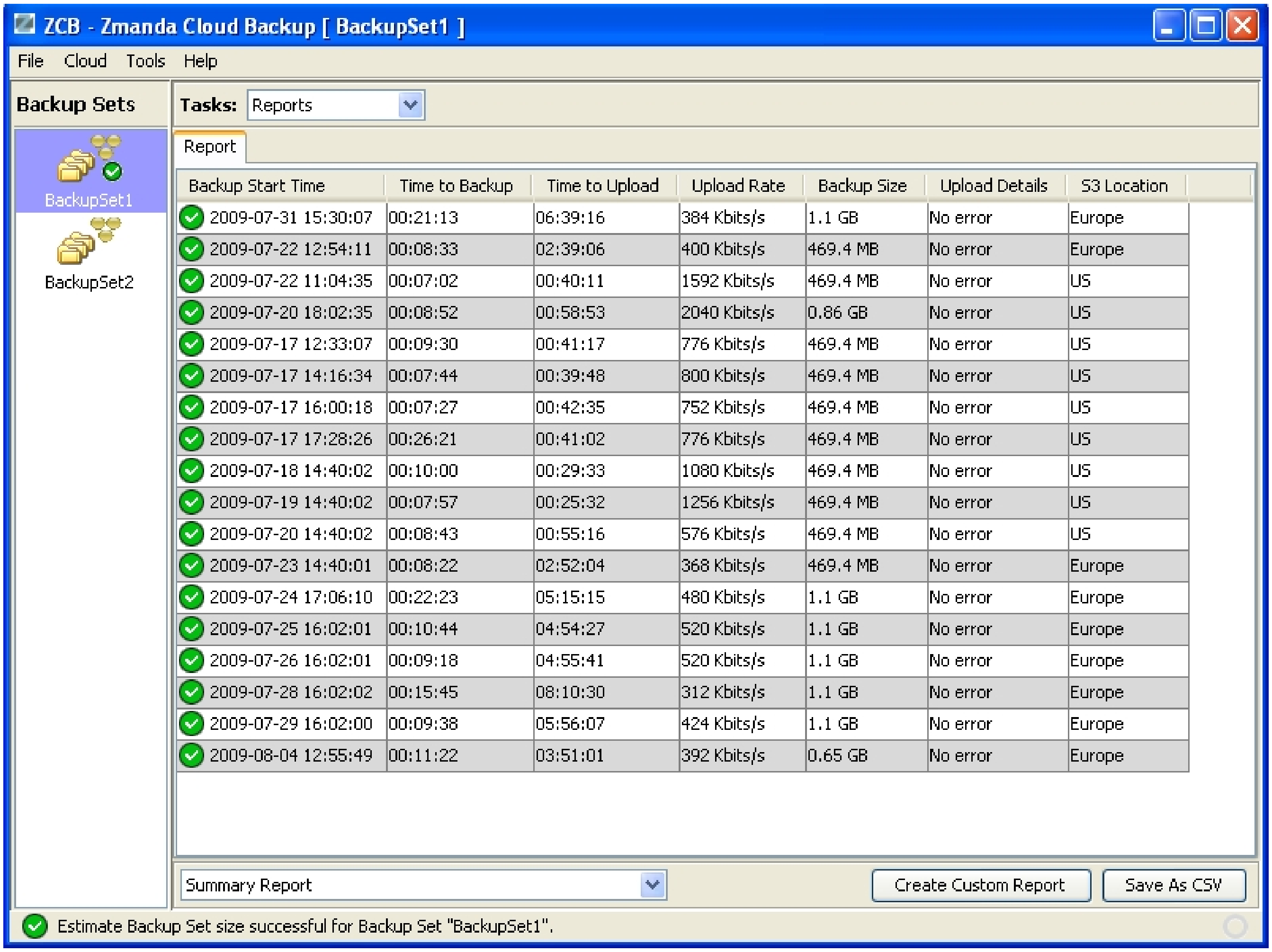
Start Time	2009-08-05 08:18:35
Status	Successful
Elapsed Time	00:02:21:29
Type Of Download	Download backup data from Amaz...
Download rate	646.43 Kbits/s
Total Download Size	0.65 GB
Total Backup Archives To Download	1
Backup Archives Downloaded So Far	1
Backup Run (Start Time)	2009-08-04 12:55:49

Restore

Start Time	2009-08-05 10:40:07
Status	Successful
Elapsed Time	00:00:07:59

Estimate Backup Set size successful for Backup Set "BackupSet1".

Choose **Reports** from the **Tasks** drop down menu to display a table of various statistics related to backup and uploads.



Tasks: Reports

Backup Start Time	Time to Backup	Time to Upload	Upload Rate	Backup Size	Upload Details	S3 Location
✓ 2009-07-31 15:30:07	00:21:13	06:39:16	384 Kbits/s	1.1 GB	No error	Europe
✓ 2009-07-22 12:54:11	00:08:33	02:39:06	400 Kbits/s	469.4 MB	No error	Europe
✓ 2009-07-22 11:04:35	00:07:02	00:40:11	1592 Kbits/s	469.4 MB	No error	US
✓ 2009-07-20 18:02:35	00:08:52	00:58:53	2040 Kbits/s	0.86 GB	No error	US
✓ 2009-07-17 12:33:07	00:09:30	00:41:17	776 Kbits/s	469.4 MB	No error	US
✓ 2009-07-17 14:16:34	00:07:44	00:39:48	800 Kbits/s	469.4 MB	No error	US
✓ 2009-07-17 16:00:18	00:07:27	00:42:35	752 Kbits/s	469.4 MB	No error	US
✓ 2009-07-17 17:28:26	00:26:21	00:41:02	776 Kbits/s	469.4 MB	No error	US
✓ 2009-07-18 14:40:02	00:10:00	00:29:33	1080 Kbits/s	469.4 MB	No error	US
✓ 2009-07-19 14:40:02	00:07:57	00:25:32	1256 Kbits/s	469.4 MB	No error	US
✓ 2009-07-20 14:40:02	00:08:43	00:55:16	576 Kbits/s	469.4 MB	No error	US
✓ 2009-07-23 14:40:01	00:08:22	02:52:04	368 Kbits/s	469.4 MB	No error	Europe
✓ 2009-07-24 17:06:10	00:22:23	05:15:15	480 Kbits/s	1.1 GB	No error	Europe
✓ 2009-07-25 16:02:01	00:10:44	04:54:27	520 Kbits/s	1.1 GB	No error	Europe
✓ 2009-07-26 16:02:01	00:09:18	04:55:41	520 Kbits/s	1.1 GB	No error	Europe
✓ 2009-07-28 16:02:02	00:15:45	08:10:30	312 Kbits/s	1.1 GB	No error	Europe
✓ 2009-07-29 16:02:00	00:09:38	05:56:07	424 Kbits/s	1.1 GB	No error	Europe
✓ 2009-08-04 12:55:49	00:11:22	03:51:01	392 Kbits/s	0.65 GB	No error	Europe

Summary Report

✓ Estimate Backup Set size successful for Backup Set "BackupSet1".

Click on any column heading to sort by that field. Right-clicking on the table heading lets you select which columns to display in the table. You can save a group of selected columns as a Custom Report, and access it again from the drop down menu in the lower left of the Reports display.

You can select a backup/upload report and use right click to perform operations on the backup job. You can:

- **Delete Backup(s)/Delete Upload(s)**: Delete backup images from the Local Folder or the cloud. This is equivalent of no retention policy.

- **Retry Uploads** : Resume failed uploads (uploads are resumed from the failed block as opposed to beginning of the image). All backup images are uploaded in terms of blocks. The default block size is 10MB.

- **Restore Backup**: Start restoration of the selected backup job.

- **Backup File List/Details**: Displays list of files in the selected backup image.

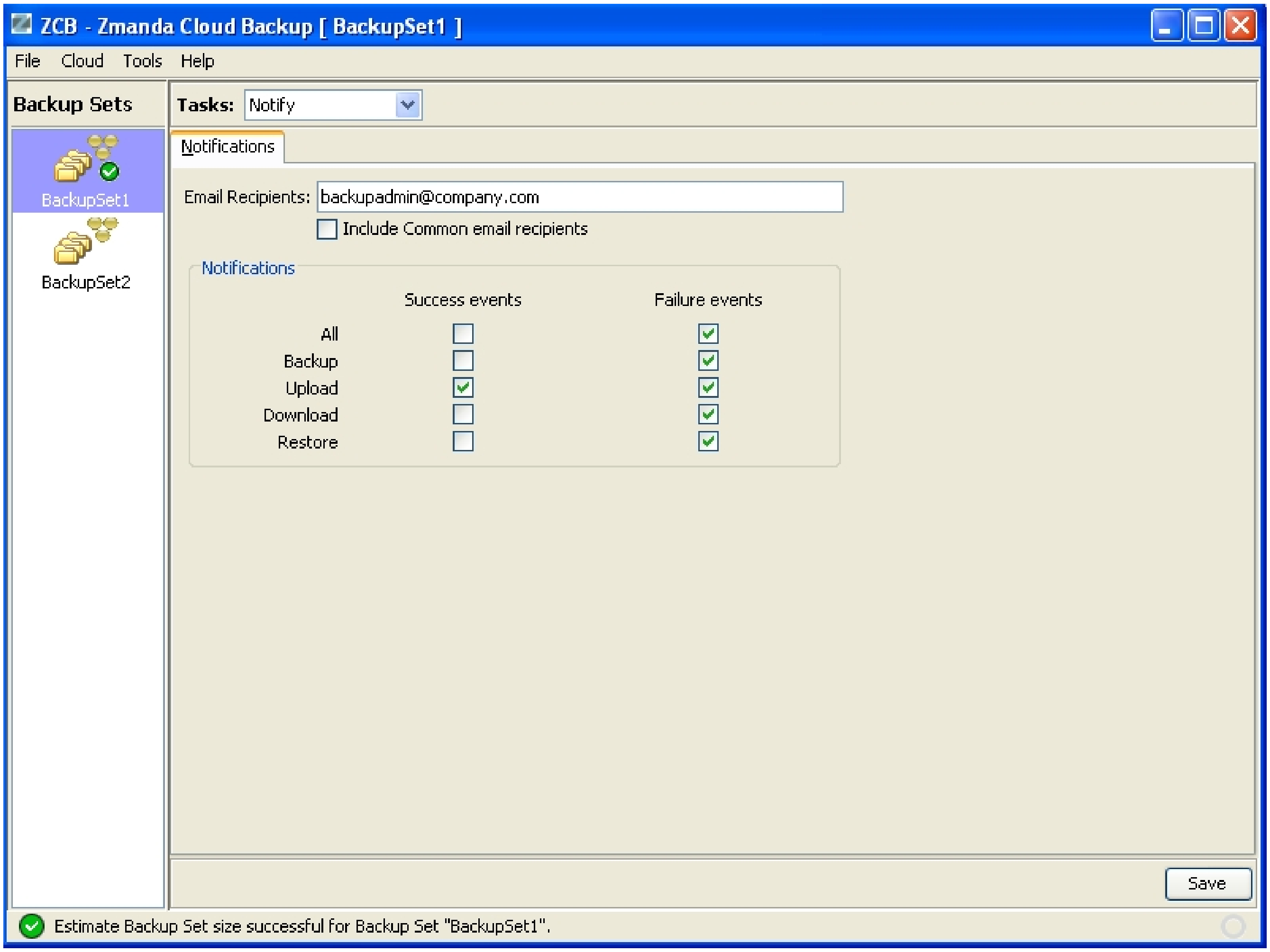
The **Save as CSV** button lets you save the displayed table as Comma Separate Values for printing, or import into other applications to create spreadsheets and charts.

Notification

ZCB provides notification of backup and recovery events in two different methods:

1. All events (successful and failure) are logged in the Windows event logs. Window event log analyzer tools can be used to filter the events and analyze them.

2. Email notification can be sent when a particular event occurs. Success and Failure backup, upload, download and restore events can be sent as an email. Administrator's email addresses can be specified for a backup set or globally. Email notification configuration can be configured in **Notify** menu item in **Tasks** drop down box. Multiple email addresses can be specified separated by ";" (semi colon) character. Common email recipients for all backup sets should be configured in **Tools > Outgoing Email Server** menu. Outgoing SMTP server must be configured for email notification to work.



Tasks: Notify

Email Recipients: backupadmin@company.com

☐ Include Common email recipients

Notifications

	Success events	Failure events
All	☐	☑
Backup	☐	☑
Upload	☑	☑
Download	☐	☑
Restore	☐	☑

Estimate Backup Set size successful for Backup Set "BackupSet1".

If you are using Exchange server, please enable **Require TLS encryption** option on the Exchange server. To configure Transport Layer Security Encryption for clients, please see Microsoft KB article http://support.microsoft.com/kb/829721

An example email reporting Upload success for backup set **BackupSetSystemState** running on server **Demo** :

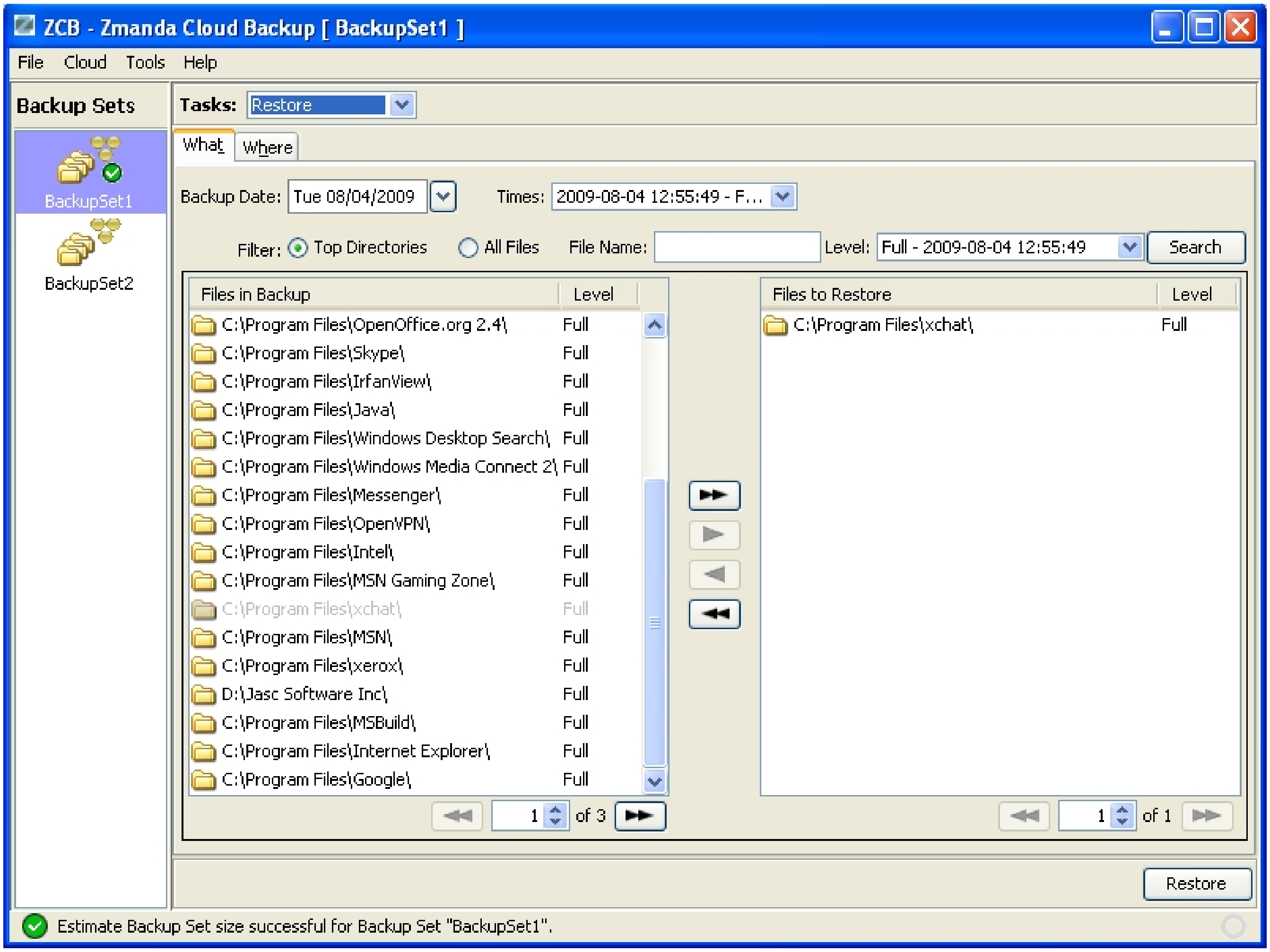
```
subject:[ZCB:demo2] Upload Report

Upload of backup set "BackupSetSystemState" is successful.

Upload start time : 2009/11/09 16:28:00
Upload end time : 2009/11/09 16:48:14
Upload Rate : 1448 Kbps
Bytes uploaded : 214.58 MB
```

```
        Error Details : No upload error
```

Restoring Files and Applications

ZCB offers a number of ways to restore file system and application backup. You can restore to the original system that was backed up using the ZCB catalog to identify a restore point. You can also restore a backup catalog originating from one system to a new system, thus allowing you to restore to that system (as for example in a bare-metal recovery scenario).

In any case, once a local catalog is available, you can choose a restore point by selecting **Restore** from the **Tasks** drop-down menu, then clicking the **What** tab.



Tasks: Restore

Backup Date: Tue 08/04/2009   Times: 2009-08-04 12:55:49 - F...

Filter: ● Top Directories ○ All Files   File Name: Level: Full - 2009-08-04 12:55:49

Files in Backup	Level
C:\Program Files\OpenOffice.org 2.4\	Full
C:\Program Files\Skype\	Full
C:\Program Files\IrfanView\	Full
C:\Program Files\Java\	Full
C:\Program Files\Windows Desktop Search\	Full
C:\Program Files\Windows Media Connect 2\	Full
C:\Program Files\Messenger\	Full
C:\Program Files\OpenVPN\	Full
C:\Program Files\Intel\	Full
C:\Program Files\MSN Gaming Zone\	Full
C:\Program Files\xchat\	Full
C:\Program Files\MSN\	Full
C:\Program Files\xerox\	Full
D:\Jasc Software Inc\	Full
C:\Program Files\MSBuild\	Full
C:\Program Files\Internet Explorer\	Full
C:\Program Files\Google\	Full

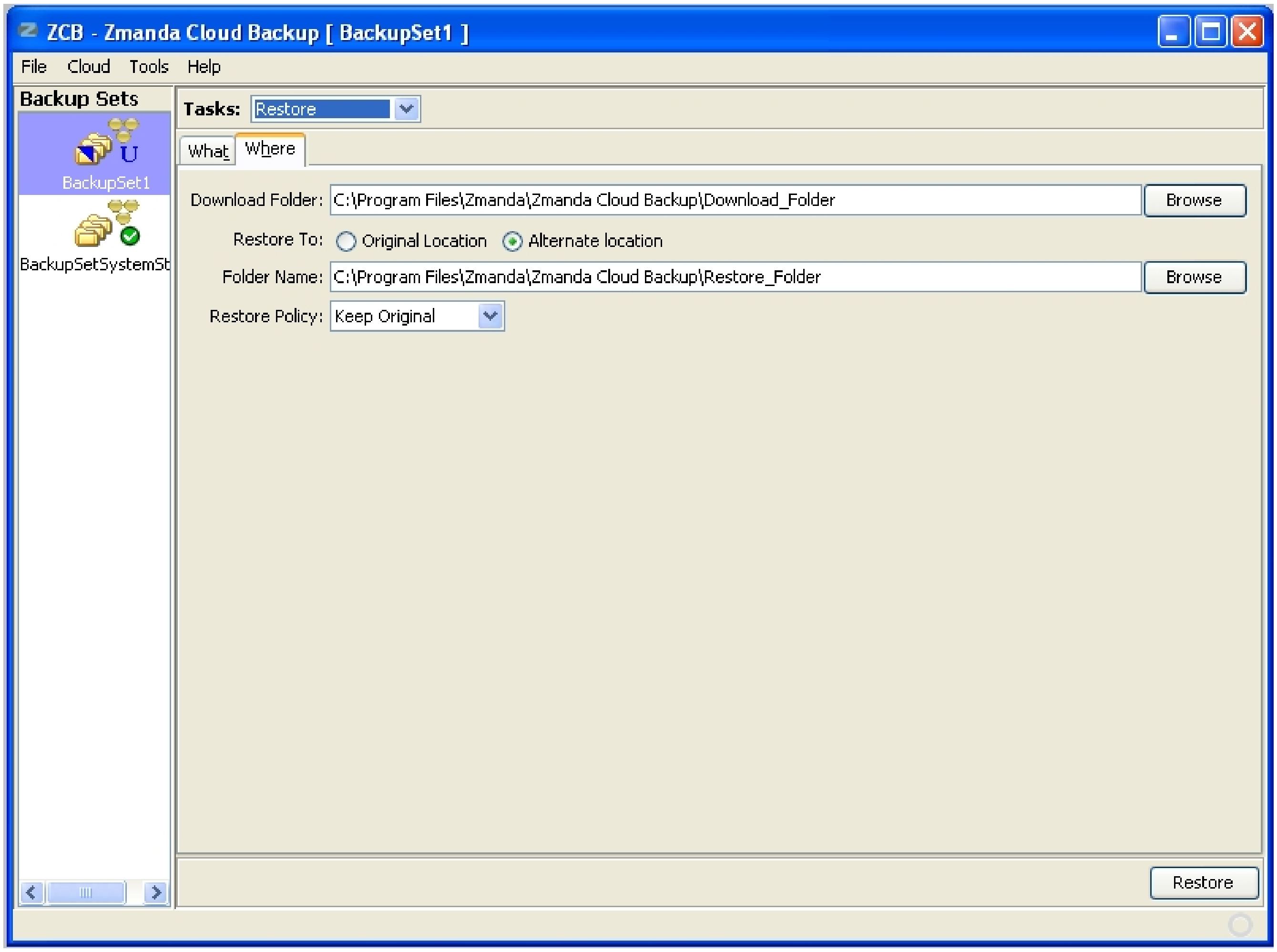
1 of 3

Files to Restore	Level
C:\Program Files\xchat\	Full

1 of 1

Estimate Backup Set size successful for Backup Set "BackupSet1".

Clicking the **Where** tab lets you choose whether to restore to the original location or some other location. To select the original location, leave the **Restore** folder empty. You can also control overwrite behavior to overwrite, rename, or retain the original file(s) by choosing the appropriate options from the **Restore Policy** menu.



Tasks: Restore

Download Folder: C:\Program Files\Zmanda\Zmanda Cloud Backup\Download_Folder

Restore To: ○ Original Location ● Alternate location

Folder Name: C:\Program Files\Zmanda\Zmanda Cloud Backup\Restore_Folder

Restore Policy: Keep Original

Next sections provide information on application specific restore procedures.

Configuring MS Exchange Restores

In the event of a server loss, how you perform the recover will depend on the server role and your disaster recovery plan. Server loss can be caused by software or hardware failure, or by the physical loss of the site where the server was housed. One would also need to recover Exchange databases in case of issues such as database corruption, loss of transaction logs, accidental deletion of mailboxes, etc. Exchange databases can be restored to the same server or to an alternate server depending on the Disaster Recovery plan decided by the Exchange Administrator.

3 types of recovery operations are allowed by Microsoft Exchange:

- roll-forward,
- point in time
- full restore

The state of the MS Exchange server when the restore is started determines what type of recovery will be available. Please see this Microsoft documentation for details on Exchange recoveries.

Here are the steps to follow to restore and recover Exchange to the original server or a different server using ZCB.

Restoring to the Original Server:

In case of Exchange database corruption or loss of the transaction log, an Exchange Administrator would want to restore the backed up data to the original Server. Before restoring the data, make sure that MS Exchange is installed on the Server and that the Databases are in the **Dismounted** state. Also make sure that the **This database can be overwritten by restore** option is selected from the Exchange System Manager (Exchange 2003) or Exchange Management Console (Exchange 2007). The Zmanda Cloud Backup automatically stops the Microsoft **Exchange Information Store** service as a pre-restore operation and will start it again once the restore is complete.

1. Open Zmanda Cloud Backup and go to the **Restore What** page. Select the backup and point in time that you want to restore.
2. On the **Restore->Where** page, choose "Restore to the original location."
3. Specify a **Folder Name** to store the data temporarily during the restore. Once confirmed, click **Restore** to start the restore process.

Important Note: After the Exchange data has been restored, ZCB automatically starts the Microsoft Exchange Information Store service. When the storage group is mounted, the Exchange store automatically replays any pending transactions using the Exchange Server soft recovery feature. Therefore all restores performed through the Zmanda Cloud Backup are always "roll-forward" restores.

Restoring to an Alternate (or Recovery) Server

There are two reasons to restore to a different machine than that from which the backup was taken:

- a disaster has destroyed the original hardware. You must restore the database to a rebuilt Exchange Server or to an alternate Exchange server.
- you are recovering an individual mailbox. In this case, there are additional steps to apply the recovery to the production Exchange server (see the next section below).

There are some pre-requisites to restore to a recovery server:

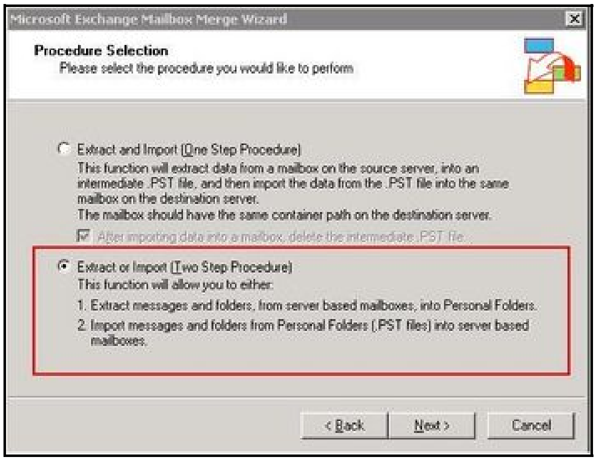
- The target server must have the same Windows OS version and Service Packs as the source server.
- Exchange must be installed and must have the same Organization and Administrative Group name as the source server.
- The storage groups and databases must already exist on the target server, and have the same names as the original storage groups or databases.
- The databases must be in the **Dismounted** state and the **This database can be overwritten by restore** option enabled through the Exchange System Manager (Exchange 2003) or Exchange Management Console (Exchange 2007).
- Because you are restoring to an alternate "recovery server" that has a different set of log files, the the signatures on the log files must match. To ensure this, either rename the **E0x.log** file located in the Transaction log directory, or enable the **Do not mount the database** option while creating a Mailbox or Public folder store.
- Zmanda Cloud Backup must be installed on the recovery server, and the backup catalog from the original server must be available. See Restoring the Backup Catalog for details.

Once you have setup the recovery server, use Zmanda Cloud Backup to recover the desired backup to the original location. Zmanda Cloud Backup automatically stops the Microsoft **Exchange Information Store** service before the restore operation and starts it again once the process is complete.

Recovering a Mailbox

To recover a mailbox, restore to a recovery server as described above, then follow these additional steps:

1. Using the Exchange System Manager, run the **Cleanup Agent** on the Mailboxes to display the restored mailboxes. Then **Reconnect** the mailbox from which you wish to retrieve the mails to its associated User account. For example, if you want to retrieve mails for user **Administrator**, then reconnect the **Administrator** mailbox to **Administrator** user account.
2. Use Microsoft's **exmerge.exe** utility to extract the mails into a PST. Use the **Two step procedure**, and select Step 1 to create the PST file.

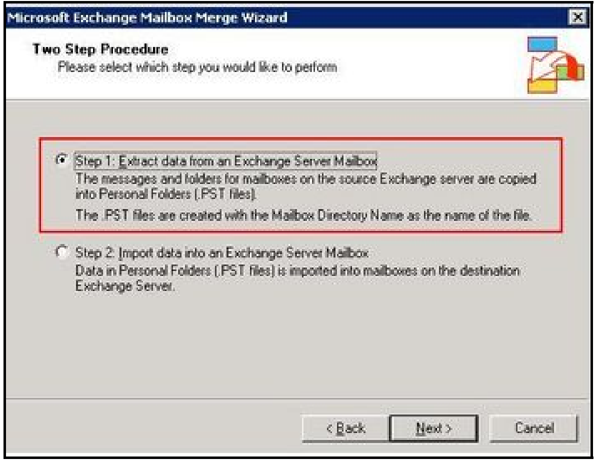


Procedure Selection
Please select the procedure you would like to perform

○ Extract and Import (One Step Procedure)
This function will extract data from a mailbox on the source server, into an intermediate .PST file, and then import the data from the .PST file into the same mailbox on the destination server.
The mailbox should have the same container path on the destination server.
☑ After importing data into a mailbox, delete the intermediate .PST file

● Extract or Import (Two Step Procedure)
This function will allow you to either:
1. Extract messages and folders, from server based mailboxes, into Personal Folders.
2. Import messages and folders from Personal Folders (.PST files) into server based mailboxes.

Running the **exmerge** utility

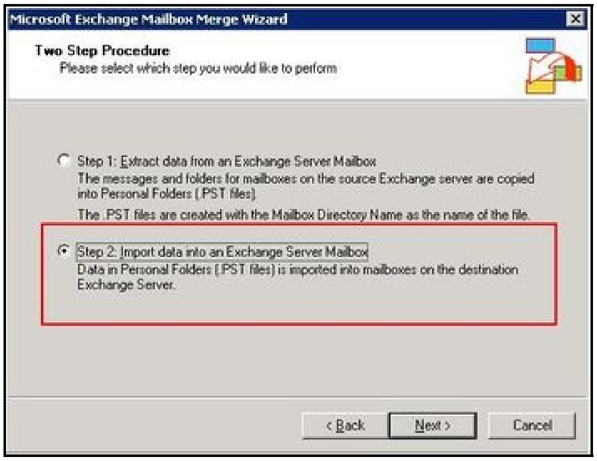


Two Step Procedure
Please select which step you would like to perform

● Step 1: Extract data from an Exchange Server Mailbox
The messages and folders for mailboxes on the source Exchange server are copied into Personal Folders (.PST files).
The .PST files are created with the Mailbox Directory Name as the name of the file.

○ Step 2: Import data into an Exchange Server Mailbox
Data in Personal Folders (.PST files) is imported into mailboxes on the destination Exchange Server.

3. Copy the PST file to the production server.
4. Run the **exmerge.exe** utility on the production server to merge the PST mails into the required mailbox. Use the **Two step procedure**, and select Step 2 to **Import** the data into an Exchange Server Mailbox.



Microsoft Exchange Mailbox Merge Wizard

Two Step Procedure

Please select which step you would like to perform

○ Step 1: Extract data from an Exchange Server Mailbox
The messages and folders for mailboxes on the source Exchange server are copied into Personal Folders (.PST files).
The .PST files are created with the Mailbox Directory Name as the name of the file.

● Step 2: Import data into an Exchange Server Mailbox
Data in Personal Folders (.PST files) is imported into mailboxes on the destination Exchange Server.

The deleted emails should now be recovered.

Restoring Microsoft SQL server

ZCB does not use VSS or SQL API for restoration. It is a simple file copy operation.

Restoration to Original location

ZCB does a restore to original location if **Original Location** is selected in **Restore > Where** page. It is the responsibility of the user to make sure that the SQL installation and database locations match with the location during backups. Since ZCB has to replace the locked database files during restoration, ZCB stops SQL Database instance services before restoration. ZCB copies the database files to the location from where they were backed up. Once the files are copied, ZCB restarts the SQL services. The SQL server will perform recovery of the databases.

Restoration to Alternate location

ZCB does a restore to alternate location if **Alternate Location** is selected in **Restore > Where** page. Alternate location should be specified as **Folder Name**. The database files from the backup are copied to this alternate location. SQL recovery is not performed and SQL services are not stopped.

Recovering Windows Oracle Databases using the ZCB and Oracle SQLplus

Recovering an Oracle database is a two-part process:

1. Use the ZCB to restore the backup to a temporary directory you create for this purpose.
2. Use Oracle's **sqlplus** program to recover the database from the restored backup files.

Before starting the restore process, make sure that the Oracle server being restored is installed in the same location as the original backup source. Oracle databases, archive log, and control file locations should also match those on the original server.

Restoring the Backup Using the Zmanda Cloud Backup

To restore a Windows Oracle database, follow these steps:

1. If necessary, install the ZCB software on the restore client (i.e. the Windows Oracle server being restored) and recover the catalog as described in Restoring the Backup Catalog.
2. Access the server with **sqlplus** (you will need the connect string). Ensure that the database is in **shutdown** state. From the **SQL>** prompt, enter the following:

   SQL>**shutdown immediate;**

3. Access the ZCB console and open the **Restore What** tab. Select point in time for the restore. Complete the restore tabs as usual.

Manually Completing the Recovery

After the Oracle databases, control files, server parameter file and archive log files are restored to the Oracle server, there are a number of manual steps you must follow to complete the database recovery. The exact steps you follow will depend on what type of backup you are recovering from, and what the recovery goals are. If you are unfamiliar with Oracle backup/recovery concepts and procedures, please review this documentation from Oracle before proceeding.

The following examples are provided to show you what the steps would be for two typical scenarios.

Example NOARCHIVELOGMODE Recovery

1. For recovery of a NOARCHIVELOGMODE backup, make two copies of the **CONTROL01.CTL** file: **CONTROL02.CTL** and **CONTROL03.CTL**. **CONTROL01.CTL** is located in the *ORAHOME\ORADATA\***DATABASE_***SID* directory). These backup control files will be used for the recovery.
2. Connect to Oracle through **sqlplus** (you will need the connect string). The **SQL** prompt is displayed.
3. Shutdown the database using this command:

   SQL>**shutdown immediate;**

4. Mount the database:

   SQL> **startup mount;**

5. Clear the redo logs:

   SQL> **alter database clear unarchived logfile "***full_path_to_redo_log***";**

   Repeat this command for all the redo log files.

6. To finish, enter the following SQL command string:

   SQL>**alter database open;**

The Oracle database is now recovered. To verify that the database is in the **open** state (read/write mode), use the following command:

```
SQL> select name, open_mode from v$database;
```

xample ARCHIVELOGMODE Recovery

1. For recovery of ARCHIVELOGMODE backups, make three copies of the **SNCF***DATABASE_SID***.ORA** file called **CONTROL01.CTL** and CONTROL02.CTL and CONTROL03.CTL. The **SNCF***DATABASE_SID***.ORA** file is located in the *ORAHOME***\product\db\database\** directory.
2. Connect to Oracle through **sqlplus** (you will need the connect string).
3. Shutdown the database by entering the following at the **SQL** prompt:

   SQL>**shutdown immediate;**

4. Mount the database:

   SQL>**startup mount**

5. Begin recovery of the control files with this SQL command string:

   SQL>**recover database using backup controlfile until cancel;**

   You are prompted for the appropriate logs (which are defined in the backup control file(s) you created in step 1); Press Enter to respond to these prompts until until the command prompt is displayed (or it errors out because it could not find a log). You may need to invoke the **recover** command multiple times to apply all the necessary logs. Enter **Cancel** when you are done to exit recovery mode and return to the SQL prompt.

6. To finish, enter the following SQL command string:

   SQL>**alter database open resetlogs;**

The Oracle database is now recovered. To verify that the database is in the **open** state (read/write mode), use the following command:

```
SQL> select name, open_mode from v$database;
```

Restoring SharePoint server

Requirements for restoring SharePoint databases to the original location on same or alternate server

1. The target SharePoint server must have the same Windows OS version and Service Packs as the source server.

2. The target server must have the same SharePoint server (WSS 3.0 or MOSS 2007) with same Service Packs and SQL server (embedded SQL server or SQL server 2005 or SQL server 2000).

3. Make sure that MS SharePoint is installed in the same location as when the backup was run. The databases and log file locations should also match the original configuration.

4. Make sure that the following services are in the **Started** state

- Windows SharePoint Services VSS Writer
- Volume Shadow Copy
- Windows SharePoint Services Tracing

Restoring to Original location and Alternate location

ZCB performs the restore to original location in following steps

1. During pre-restore operations, the following SharePoint services are stopped:
   - Windows SharePoint Services Administration
   - Windows SharePoint Services Search
   - Windows SharePoint Services Timer
   - Office SharePoint Server Search
   - IIS Admin Service (if entire farm is being restored)

2. The selected SharePoint database/s and log file/s are restored to their original location. If all the data is selected from the **Restore What** page, all the databases and Index search files are restored. You can also select individual content databases to restore.

3. During the post restore phase, the ZCB calls the SharePoint VSS writer post-restore operation which automatically detaches and then reattaches each database to the farm. This synchronizes the respective databases with the SharePoint farm.

4. The services which were stopped before the restore operation are restarted.

When restoring to an alternate location, services are not stopped and started before and after restore. Also, the SharePoint Writer's port-restore operation is not called. The selected databases and log files are simply restored to the given location.

Content Recovery

Content recovery applies to being prepared for accidental updates or deletions of data, usually by end users such as deleting documents, tasks, calender items, etc. Content recovery can be done by restoring Web application's Content databases. Since, ZCB does not support Roll-forward restore, if the restore is targeted to the original location, changes done after backup will be lost. So, one can restore the respective Web application's content databases to alternate location and use Third Party tools to extract the required object.

Web application Recovery

A web application recovery would be required in case of accidental deletion or corruption of the content databases, etc. To recover a deleted/corrupted web application's content database to Original server, select the appropriate database files from SharePoint server backup.

Disaster Recovery

Disaster recovery operations are performed only when a fatal disaster occurs, which usually involves replacement of hardware and sometimes re-installation and setup of software. A Disaster recovery requires a full server data restoration.

Backup plan for Disaster recovery includes backing up System State, C:\Windows directory (since System State does not include all files from C:\Windows), SharePoint Installation directory, SharePoint Server databases & files, Web application pool directories from C:\Inetpub. Create separate backup sets for each of the above components in the ZCB **Backup What** page.

Disaster recovery should be performed in following order:

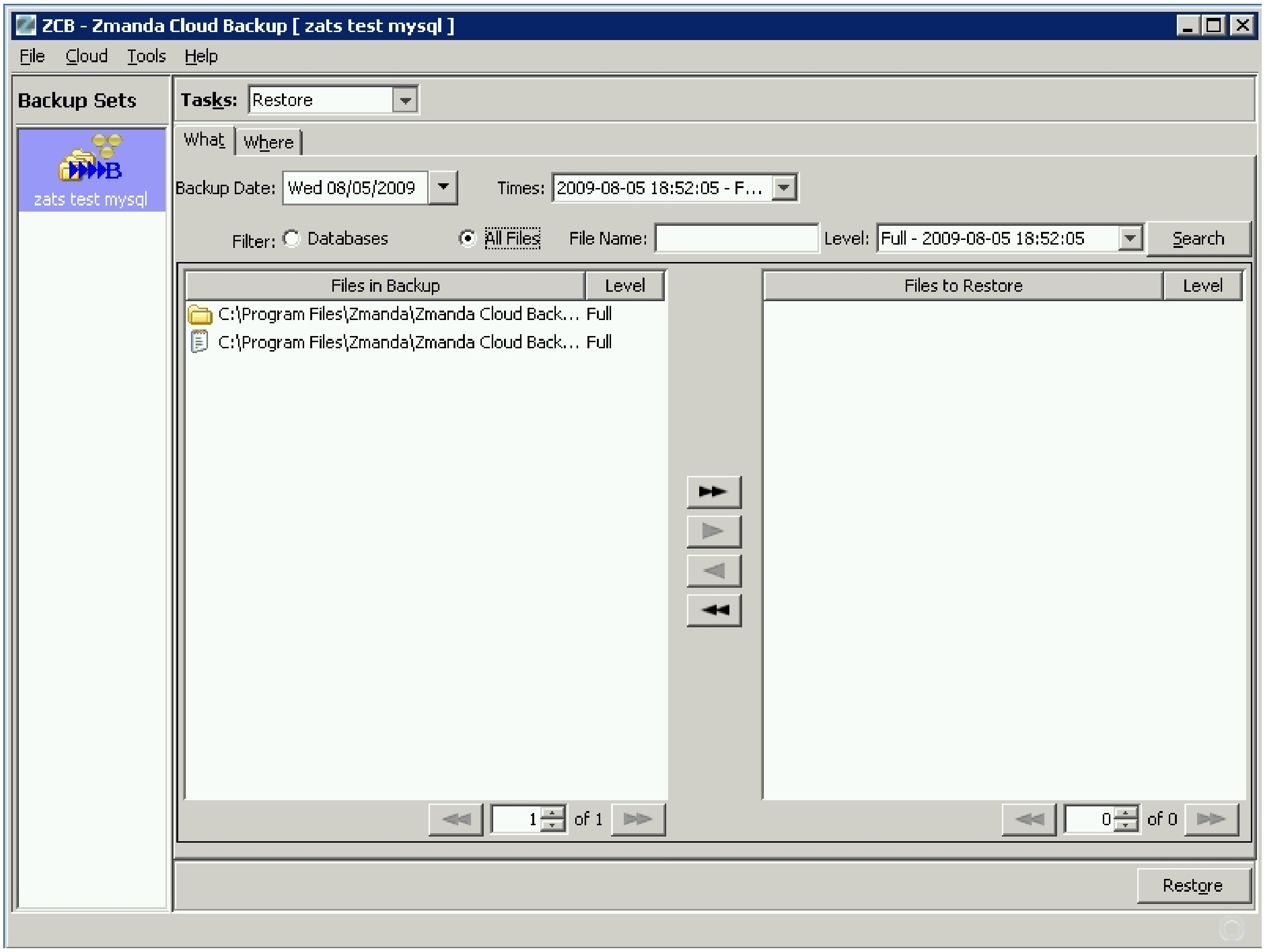
1. Install Windows Operating System with the same Service packs as original server. Do not install SharePoint server.

2. Select the "System State" backup set full backup from ZCB and restore it to Original location. Do not reboot the Server after System State restore.

3. Then restore the backup data from "C:\Windows", "SharePoint Installation directory", "SharePoint Server databases & files" and Web application pool directory i.e. C:\Inetpub.

4. Reboot the Server. SharePoint server should be running on the system.

Restoring MySQL databases/tables



Tasks: Restore

Backup Date: Wed 08/05/2009

Times: 2009-08-05 18:52:05 - F...

Filter: ○ Databases ● All Files

File Name:

Level: Full - 2009-08-05 18:52:05

Files in Backup	Level
C:\Program Files\Zmanda\Zmanda Cloud Back...	Full
C:\Program Files\Zmanda\Zmanda Cloud Back...	Full

1 of 1

Files to Restore	Level

0 of 0

Users can select which database(s) or table(s) to restore (Select **Databases** filter) or the backup files to restore (Select **All Files** filter). Depending what the backup images contain, the database filter allows user to select **All Databases**, **Selected databases** (list of databases are displayed in the left pane) or **Selected Tables** (the list of tables in the backup image are displayed in the left pane). The **All Files** filter shows the backup file (*backup.sql*) containing SQL commands to recreate the MySQL backup set.

The MySQL server information and MySQL user credentials for the backup set (See **Backup What** page) is used for restoration when the backup image is being restored to **Original location** (see **Restore Where** page). The MySQL user should have necessary privileges to perform MySQL operations that the backup image contains. Restoration process requires MySQL client commands to be installed on ZCB machine and it must be compatible with the MySQL server version. MySQL server must be running for restoration to be successful.

MySQL database/table restoration is performed in two steps: The backup image containing SQL commands is restored to the location specified in Restore Where page. The **Restore Policy** in the **Restore Where** page is applied to the files in this location (not MySQL databases/tables). The *mysql* client command is used to execute the SQL commands that are in the backup image in the second step. The **Restore To** and **Restore Policy** values are not considered in the second step.

When MySQL database(s) or file(s) are being restored to **Alternate location**, no MySQL recovery is performed. The MySQL backup image contains sequence of MySQL commands that can bring the database back to original state. Restoration to Alternate location allows users to edit the SQL commands in the backup files as needed.

Cloud Menu

Checking the S3 Connection and Subscription

To verify that S3 storage is available, choose **Cloud > Check Amazon S3 Connection.** This causes ZCB to connect to S3 and validate the purchased Amazon S3 certificate. You can use this test to validate your installation, or to troubleshoot failed uploads/downloads.

Purchasing and Managing S3 Storage

Choose **Cloud > Purchase Subscription** or **Cloud > Manage Subscription** to open a browser window that connects you to Zmanda Network and Amazon portal, where you can login to see the storage you have purchased, and purchase additional storage if desired. Zmanda Network account information and Amazon account information is required to access the information.

Displaying billing information

To track display a report that shows what you are spending on the cloud storage, click **Cloud->S3 Billing.** This takes the user to Amazon web site that provides detailed billing information for current month as well as prior month. Amazon account information is required.

Importing Amazon S3 certificate

After purchasing Amazon S3 subscription, S3 certificate will be available in your Zmanda Network account.

The certificate file must be downloaded to ZCB machine and imported into ZCB using **Cloud > Import Cloud Certificate** The dialog window allows users to select the certificate file. The certificate file must be called **s3.crt** and there can be only one certificate installed for a ZCB installation.

Tools Menu

Refreshing the Display

Choose **Tools > Refresh** to update ZCB displays (especially the Monitor display) with the latest information.

Collect Logs

If you run into a problem that requires assistance, choose **Collect Logs** from the ZCB **Tools** menu before contacting the Zmanda Support Team. ZCB then collects all the relevant files into an archive, displaying its name and location. Be patient; collecting the logs can take a few minutes. Attach the log file to your support request.

Collect Logs has to be run as an user with Administrator privileges. If ZCB UI is being run as an user who is not an Administrator on Vista, Windows 7 or Windows 2008 server, an user credentials dialog is popped up asking to enter Administrator or any other user name with Administrator privileges and password. In Windows XP and 2003 server, if ZCB UI is being run as an user who is not an Administrator, Collect logs will not work. You will have right click on the ZCB support short-cut and use **Run as** option and enter Administrator credentials.

Restoring the Backup Catalog

The backup catalog is what ZCB uses to index data for point-in-time recovery. To restore data to a machine that was never backed up by ZCB (as in a "bare metal" recovery) requires that your first recover the backup catalog by clicking **Tools > Restore Catalog.** This procedure should be used in case the ZCB machine completely fails.

Mail notification

For ZCB to send email notifications, outgoing SMTP server and valid user credentials must be specified. This information can be specified by clicking **Tools > Outgoing Mail Server.** Email recipients common to all backup sets who have to be notified can be specified in this dialog. For example: If you are using Gmail SMTP server to send emails, set **SMTP server** as smtp.gmail.com, **Sender Email Address** as your gmail address, **Password** as gmail user password and **Port** as 467.

ZCB services

ZWC services are background services that provide ZCB functionality. These services can be restarted by clicking **Tools > Restart ZWC service.**

Advanced Options

ZCB uses TCP ports 10080 and 10081 for backups and restoration. If these ports are not available at the time of installation, next available ports are selected.
ZCB also has the provision of changing the ports by using **Tools > Advanced Options**. One can specify the "Backup" and "Restore" ports and click on Save.
ZCB services are restarted to apply these port changes.

Setting the Log verbosity

Choose **Tools->Log level** to set the severity of errors that will be logged. The least verbose level (**Error**) generates smaller logs but less information. For most situations, a log level of **Warning** (Default value) is appropriate. Zmanda Support may ask you to set the log level to **Debug** when helping you troubleshoot problems.

Backup encryption

ZCB uses industry-standard RSA RC4 algorithm for backup encryption. RC4 is RSA's standard streaming encryption algorithm. ZCB supports Windows PFX (Personal Information Exchange) certificates only. Please note that this certificate is different from Amazon S3 certificate downloaded from Zmanda Network.

The backup archive stores all encryption metadata information in encoded form including the certificate that was used to encrypt. The SHA1(secure) hash of the certificate is also stored in the archive.

ZCB can decrypt the backup image only if the encryption certificate (in the same form during backup) is present on the target machine. A renamed certificate of the same form will also be able to decrypt the files. User will be able to view the files (filenames) stored within the archive through Winzip and PKZIP Windows utilities, but will not be able to decrypt through these utilities. Only ZCB can decrypt the backup files.

The certificate to be used for encryption must be in **amandabackup** user's **Personal** Certificate Store as well as **Trusted Root Certification Authorities** (irrespective of which Windows user uses ZCB). Validation of the backup set will fail if the encryption certificate specified in the backup set is not in the certificate stores. The procedure to add the certificate to certificate store is described in next two sections.

ZCB uses **Zmanda** key container to manage the private keys associated with **amandabackup** user. When **amandabackup** user is deleted (Uninstalling ZCB software without saving configuration and data) or in Disaster Recovery situation, it is important to export the **Zmanda** key container and import it in the new machine. Exporting/Import Key container section discusses this procedure.

The ZCB user **amandabackup** must have “Full Control” permissions on the following folders so that it can create **Zmanda** key container during backup encryption process.

On XP and Windows 2003:

```
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys
```

On Vista, Windows 2008 and Windows 7:

```
C:\Program Data\Microsoft\Crypto\RSA\MachineKeys
C:\Program Data\Microsoft\Crypto\RSA\
```

Exporting a certificate

You need to export the certificate to file if you do not have certificate **pfx** file. From the Windows **Start** menu, click **Run** and enter

certmgr.msc

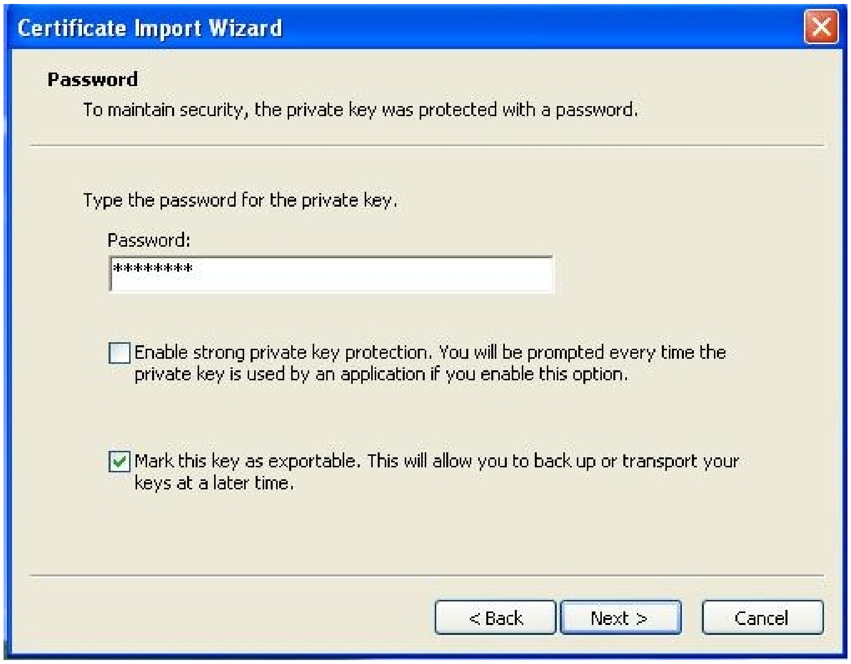
Find a certificate to export, double-click it, then click **Details**. Choose the **Copy To File** option, which will let you select a location for the exported certificate. When exporting the certificate, make sure that:

- the **Yes, export the private key** option is checked
- the **Delete Private Key if export is successful** option is left unchecked

After the file has been saved, close the **certmgr.msc** utility. The exported certificate should be in a folder that is accessible by the **amandabackup** user.

Importing the certificate for amandabackup user

Log on to the ZCB machine as the **amandabackup** user and import the certificate by double-clicking it from the file manager. Double clicking the certificate *pfx* file will start the **Certificate Import Wizard**. The password used to protect the private key must be entered. Make sure the **Mark this key as exportable** option is selected. See the screen figure below. Place it in a certificate store. It should be in **Personal** certificate store.



Password

To maintain security, the private key was protected with a password.

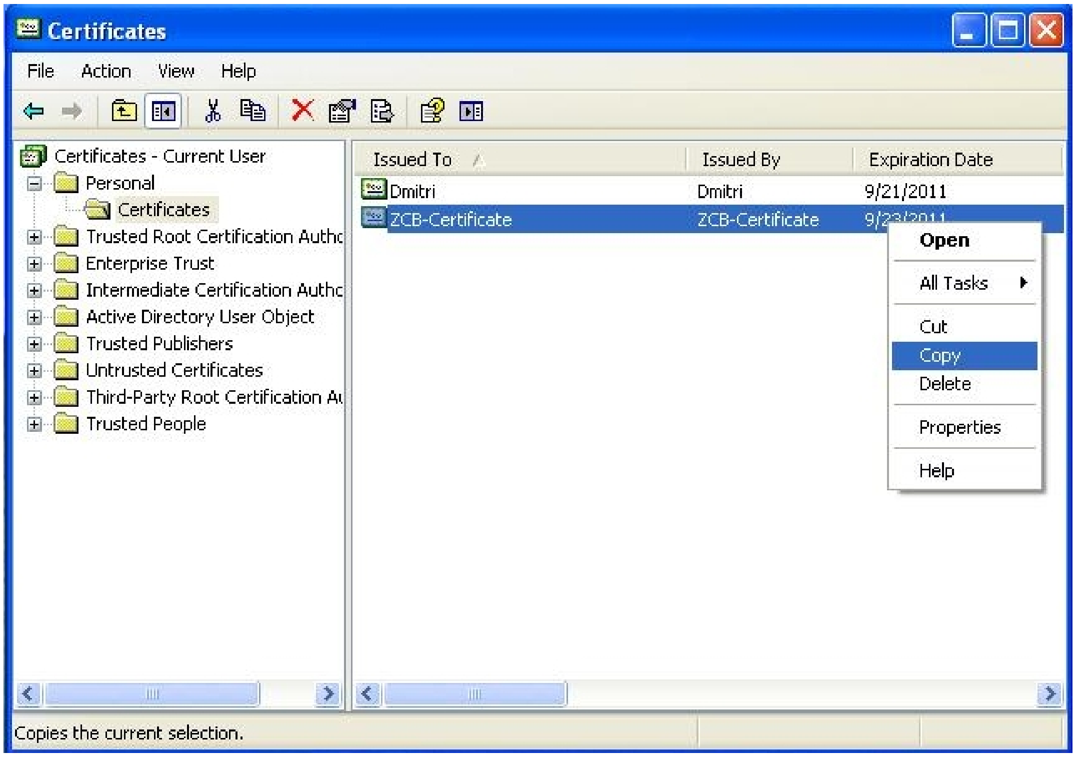
Type the password for the private key.

Password: ********

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

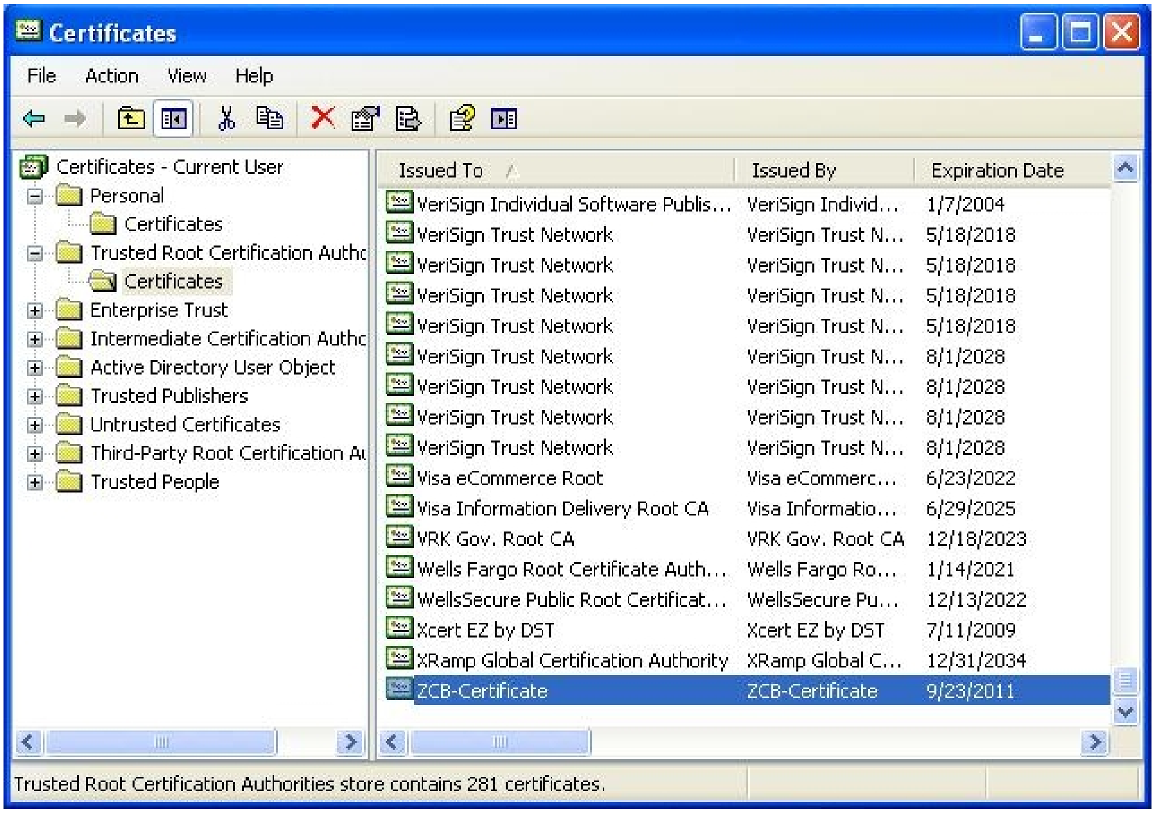
From Windows **Start** menu, click **Run** and enter **certmgr.msc** to browse the certificate store. Browse Personal Certificate Store certificates (See screen figure below) and copy the imported certificate (right click menu) from the **Personal\Certificates** folder to the **Trusted Root Certification Authorities\Certificates** folder to inform the system that the newly imported certificate is a trusted one.



Issued To	Issued By	Expiration Date
Dmitri	Dmitri	9/21/2011
ZCB-Certificate	ZCB-Certificate	9/23/2011

Copies the current selection.

The certificate will be in both Personal Certificate Store and Trusted Root Certification Authorities as shown below.


Certificates
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authc
Certificates
Enterprise Trust
Intermediate Certification Authc
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People

Issued To	Issued By	Expiration Date
VeriSign Individual Software Publis...	VeriSign Individ...	1/7/2004
VeriSign Trust Network	VeriSign Trust N...	5/18/2018
VeriSign Trust Network	VeriSign Trust N...	5/18/2018
VeriSign Trust Network	VeriSign Trust N...	5/18/2018
VeriSign Trust Network	VeriSign Trust N...	5/18/2018
VeriSign Trust Network	VeriSign Trust N...	8/1/2028
VeriSign Trust Network	VeriSign Trust N...	8/1/2028
VeriSign Trust Network	VeriSign Trust N...	8/1/2028
VeriSign Trust Network	VeriSign Trust N...	8/1/2028
Visa eCommerce Root	Visa eCommerc...	6/23/2022
Visa Information Delivery Root CA	Visa Informatio...	6/29/2025
VRK Gov. Root CA	VRK Gov. Root CA	12/18/2023
Wells Fargo Root Certificate Auth...	Wells Fargo Ro...	1/14/2021
WellsSecure Public Root Certificat...	WellsSecure Pu...	12/13/2022
Xcert EZ by DST	Xcert EZ by DST	7/11/2009
XRamp Global Certification Authority	XRamp Global C...	12/31/2034
ZCB-Certificate	ZCB-Certificate	9/23/2011

Trusted Root Certification Authorities store contains 281 certificates.

Exporting/Importing **Zmanda** Key container

Encryption Metadata for the association between *amandabackup* user and the digital certificate used is stored under the **Zmanda** key container on disk on the backup client machine.

It is important to export the key container before uninstalling ZCB on the client machine. Also, this key container will be needed, in the case of restoring encrypted archives on a different restore machine.

The exported XML file is needed for disaster recovery and must be backed up. To export and import key containers, .NET (version 2.0 or greater) framework must be installed in the ZCB machine. It is usually found under *C:\WINDOWS\Microsoft.NET\Framework and Framework64* folders.

To export the **Zmanda** key container to XML file, run the following command (Windows Start > Run > command)

```
aspnet_regiis -px “Zmanda” “<Name of XML file to be created>” -pri
```

IMPORTANT: Before importing **Zmanda** key container from another machine, make sure you have exported **Zmanda** key container from the current machine. This step is necessary if you are importing **Zmanda** Key container into a machine that is already performing ZCB encrypted backups. Use the above procedure to export **Zmanda** key container. To import the **Zmanda** key container from the XML file, run the following command (Windows Start > Run > command)

```
aspnet_regiis -pi “Zmanda” “<Name of the exported XML file>” -exp
```

You will need to import the exported key container from the current machine, in order to recover from encrypted archives backed up from this machine. After importing the **Zmanda** key container, the digital encryption certificates have to be imported for the **amandabackup** user. This is necessary to recover from encrypted archives.

Location of Log Files

Log files created by the ZCB program are stored in the **\Debug** directory installed along with ZCB (Typically **C:\Program Files\Zmanda\Zmanda Cloud Backup\Debug**). **LogFile.txt** is ZCB engine log file. **ZIBLogFile.txt** is the log file for the ZCB program itself.

Log files for the installation and uninstallation process can be found in "%temp%" folder which is typically at **"C:\Documents and Settings\<Logged_in_user>\Local Settings\Temp”** for most systems. If not, it resides in the Windows Installation drive (D:, E: ...)under the same directory structure.

ZCB installer creates a file named "ZCBInstallLog.log" as system-log of the installation process in the %temp% folder

These logs are collected as part of Tools->Collect Logs operation.

ZCB also logs successful and failed backup, restore, upload and download events to Windows Event Logs.

Trademark Notices