

User Guide - Google Cloud - English - v4.8

Table of Contents

- Table of Contents
- Introduction to ZCB
- User Manual
 - Overview
 - Supported Backup Types
 - System Requirements
 - Installation
 - Installation
 - The amandabackup user
 - Importing the ZCB certificate
 - Unattended installation
 - Configuration
 - Backup Sets
 - Backup Levels
 - Full, Differential, or Incremental Backups?
 - Working with Backup Sets
 - Configuring Backup Sets
 - Backup What
 - Backup Where
 - Backup to Cloud
 - Backup to Disk
 - Backup to both disk and cloud
 - Upload from disk to cloud
 - Cloud Storage Options
 - Local Disk Storage Options
 - Retention policies
 - Bandwidth Throttling
 - Secure Transfer (SSL)
 - Backup How
 - Compression
 - Encryption
 - Backup When
 - Pre-backup and Post-backup Actions
 - Email Notification
 - Scheduling
 - Performing Backups
 - Windows File System
 - Microsoft SQL server
 - Microsoft Exchange Server
 - Microsoft SharePoint
 - Windows System State
 - MySQL Server
 - Oracle Server
 - Hyper-V
 - Monitoring
 - Reporting
 - Report History
 - Manage Report History
 - Report Templates
 - Verify Backup Data
 - Task Management
 - ZCB Global Dashboard
 - Restore
 - Overview
 - What is a Backup Catalog?
 - Restore to the original machine
 - Restore to a different machine
 - Restore Options
 - Advanced Filtering
 - Restore the Windows File System
 - Locate A Backed Up File
 - Restore a Microsoft SQL server
 - Requirements for all database restores:
 - Additional requirements for restore to another machine

- Special Options for database restores:
- Database Ownership After Restore
- Restore locations
 - Original Location
 - Restore a Copy of Database to Original or New Location
 - Restore to a New Location and Overwrite Original Database
 - Restore to an alternate location without Recovery (FULL Backups Only)
- Restore a Microsoft Exchange Server
- Restore Microsoft SharePoint
- Restore Windows System State
- Restore a MySQL Server
- Restore an Oracle Server
- Restore Hyper-V
- Locate A Backed Up File
- Advanced Filtering
- Disaster Recovery
 - Preparing for Disaster Recovery
 - Performing Disaster Recovery
- Administration
 - Advanced Options
 - Data Transfer and Networking
 - Retention Policy Enforcement
 - General
 - Localization
 - Email Notification
 - Global Email Notifications
 - Backup-set Specific Email Notifications
 - Purge All Backup Runs Before...
 - Upgrading ZCB
 - Reinstalling ZCB
 - Cleaning up ZCB installation
 - Cloud Storage
 - Checking the Cloud Connection and Subscription
 - Managing Amazon S3 Storage
 - Managing Google Cloud Storage
 - Import Cloud Certificate
 - Restore Catalogs
 - How to restore the backup catalog
 - Restore Catalog from Cloud
 - Restore Catalog from Local Directory
 - Moving local backup data to a different location on the same machine
 - Changing Log Level
 - Collect Logs

Introduction to ZCB

ZCB is the complete backup solution for Windows servers. It backs up file systems and live applications such as Microsoft Exchange and SQL Server to a highly dependable storage cloud – Google Cloud Storage.

User Manual

Overview

Supported Backup Types

ZCB can back up files, system state, and several live applications.

- Windows NTFS files and folders
- Windows ReFS files and folders
- Microsoft SQL Server 2000, 2005, 2008, and 2012
- Microsoft Exchange Server 2003, 2007, 2010, and 2013
- Microsoft SharePoint Server 2007/WSS 3, 2010, and 2013
 - Standalone and Single-Server Sharepoint Farm Configurations are supported.
 - Multi-server Sharepoint Farm Configurations are not supported.
- Windows System State (including the registry, certificate server, and active directory information)
- MySQL Server 5.x

- Oracle Server 11i, 11g, or later.
- Hyper-V (Windows 2008, 2012, and 8 only)
 - Server "core" installations are not supported for Windows 2008 or 2012

SQL Server, Exchange Server, SharePoint, and Hyper-V server configurations are automatically discovered by ZCB.

System Requirements

Your system must meet the following requirements:

- **Windows Version**
 - Windows XP (Home or Pro) with SP2 or higher.
 - Windows Vista.
 - Windows 7.
 - Windows Server 2003 SP3.
 - Windows Server 2003 R2.
 - Windows Small Business Server 2008.
 - Windows Server 2008.
 - Windows Server 2008 R2.
 - Windows Small Business Server 2011.
 - Windows 8.
 - Windows Server 2012.
- **Hardware**
 - Dual-core CPU.
 - 2GB of memory.
 - Free disk space for snapshots, metadata, and general performance.
 - Up to 20% free space on the drive which ZCB is installed.
 - Up to 20% free space on the drive(s) to be backed up.
- **Dependencies**
 - Java 7 is required for all Zmanda Cloud Backup installations.
 - Backups of Microsoft Exchange Server 2007 have additional dependencies:
 - .NET Framework 4.0 or higher
 - Powershell 2.0 or higher. Powershell is available as part of the [Windows Management Framework](#).
 - The **Check Dependencies** option in the Tools menu can be used to verify if the proper dependencies are installed on the system.
- **Other Requirements**
 - The language selected in the ZCB Installer and the ZCB program must match the Windows system locale.
 - The Remote Registry Service must be enabled before installation.
 - The Volume Shadow Copy Service (VSS) must be enabled. Although the Volume Shadow Service is enabled by default, it may have been turned off after Windows installation.
 - To ensure that VSS is running:
 - Right-click the **My Computer** icon and choose **Manage** from the pop up menu.
 - Expand the Services and Applications tree and locate the **Volume Shadow Copy** Service. If it is not started, change the General Properties to make the Startup Type **Automatic**.
 - ZCB must be installed and all ZCB operations must be performed as a user that has Administrator privileges.
 - ZCB requires access to TCP Ports 10080 & 10081, which are default ports used by ZCB for backup and restore.
 - Alternate ports can be specified. Please refer to the [Advanced Options](#) section in this document.
 - The ZCBService requires access to Port 10085. If port 10085 is not available, please see [How to change the default port used by the ZCBService](#).

Installation

ZCB installation involves two steps – installation of the software and importing the ZCB cloud certificate. Product downloads (32-bit and 64-bit) and the cloud certificate are available on the [Zmanda Network Downloads](#) screen.

If the product downloads and/or the cloud certificate are not available for download, please see [Purchase & Payment Verification Errors](#).

Installation

ZCB uses the InstallShield installer and self-extracting **.exe** files for installation. After downloading, double-click the install file to begin installation. The installer will check for system requirements, such as the JRE, before installation.

The *amandabackup* user

Upon installation, ZCB creates a new user named *amandabackup*. For fine-grained access control, ZCB uses *amandabackup* for performing all backup related tasks.

For more information about *amandabackup*, please see [What is the amandabackup user?](#)

Importing the ZCB certificate

Once ZCB is installed, download the certificate from the Zmanda Network **Downloads** screen. Be sure to use the save as option and name the certificate *cloud.zmanda*. Once downloaded, import the certificate into ZCB using the **Cloud > Import Cloud Certificate** menu option.

The certificate has to be downloaded and imported into each ZCB instance you have running. You can use different ZCB certificates if you want to use different Google accounts.

Unattended installation

If you are planning to install ZCB on multiple machines, you should record the user input for playback. The recorded user input can be used to install ZCB by command line on multiple machines in an unattended manner. Depending on user privileges, the command prompt may need to be run as Administrator.

The recording file will contain all user input for playback. To write a recording file for installation, use the command: **setup.exe /r /f1 "<filename.iss>"**

To write a recording file for uninstallation, use the command:

setup.exe /r /removeonly /f1 "<filename.iss>"

The ZCB installer can read the user input recorded file from the same directory. Alternate location for user input can be provided using the /f1 option. The installation log file will be created in same directory (default: Setup.log). Alternate location for the log can be provided using the /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 finish before the installation or uninstallation process is completed. Use the /WAIT flag if you want the setup.exe command to wait for the process to be completed. For example: The following installation command will wait until the process is complete in the Windows prompt

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 for unattended installation and uninstallation. These setup files assume that

1. ZCB will be installed in the **C:\Program Files\Zmanda\Zmanda Cloud Backup** folder. You will be asked to provide a password for the **mandabackup** user. Please note this password as it may be required for advanced configurations!
2. ZCB uninstallation will not preserve configuration data

Furthermore, utilities are provided to import and export existing ZCB configurations, to easily transfer backup sets to new machines.

Export_ZCBConfiguration.bat will export an existing configuration into a .zip file, which can then be used to automate the installation of ZCB on new machines. Export_ZCBConfiguration.bat is located in C:\Program Files\Zmanda\Zmanda Cloud Backup\bin/.

- Run the file from the command prompt.
- You must specify the export location from the command prompt as well.
- For example, to export to C:\Export_Folder you would enter
 - C:\Program Files\Zmanda\Zmanda Cloud Backup\bin\Export_ZCBConfiguration.bat C:\Export_Folder
- A file named "ZCB.zip" is now in C:\Export_Folder

Import_ZCBConfiguration.bat will import the ZCB.zip folder created by Export_ZCBConfiguration.bat

The import script needs access to the exported ZCB.zip file. Copy it to a local folder or provide path to the network share.

- Make sure that there are no existing backup sets on the new machine to avoid any conflicts during the import process.
- Open the command prompt and run **Import_ZCBConfiguration.bat** from the /bin/ directory.
- The following example uses the same destination folder as above.
 - C:\Program Files\Zmanda\Zmanda Cloud Backup\bin\Import_ZCBConfiguration.bat C:\Export_Folder

On successful completion of the import process, open the ZCB UI to make sure that all the backup sets, their respective schedules and configurations such as Backup Folder, Local & Cloud Retention period, Compression, etc are correctly imported to the new machine.

Note: The Backup Folder for the local storage will be modified depending on a target machine's operating system if default path is used. On the other hand, if the user modifies this location when they create a backup set template, then ZCB on all the other machines will have the same modified location.

- Validate the Backup Set before running backups to make sure that all the configurations are in good shape.

Configuration

Backup Sets

A backup set defines the parameters (the what, how, where, and when) for backing up a group of directories or an application. Each backup set can only be of a single type. For example, you cannot back up an Exchange server and Windows System state in the same backup set. Instead, you must create a new backup set for each type of backup.

Backup set names are limited to 32 characters. You cannot use Windows reserved characters, such as `/|?_<>*:+&-`.

Backup Levels

ZCB supports full, differential and incremental backups.

Full backup: This type of backup makes ZCB back up **all** of the data associated with the backup set. Full backups are also referred to as backup level 0.

Differential backup: This type of backup makes ZCB back up **only** the data which changed since the *last successful full backup*. This is also referred to as backup level 1.

Incremental backup: This type of backup makes ZCB back up **only** the data which changed since *the last successful full, differential, or incremental backup*. This is also referred to as backup level 2 (or more).



While differential and incremental backups help reduce the time and size of backup runs, they also create dependencies between different backup runs.

For a full restore of **all** data, ZCB will need all the dependent backup runs.

For a restore of **some files** in a File System Backup, ZCB can restore files contained within a specific incremental or differential backup without needing access to any other dependent backups.

Incremental backups are generally much smaller in size than differential backups but can make the restore process slower over a period of time. Differential backups, on other hand, offer a good tradeoff between "time to backup" and "time to restore". To reap the benefits of both incremental and differential backups, you may combine both types in a single backup set.

A backup set that mixes both incremental and differential backups may look like this:

- Do a full backup every 3 months
- Do differential backups every month
- Do incremental backups every day

Full, Differential, or Incremental Backups?

Your first backup should be a Full backup. Once it is complete, you can use Differential or Incremental backups to reduce the time and size of your future backup runs.

Please see [What are Incremental and Differential backups?](#) for more information on different backup levels.

Working with Backup Sets

Backup sets are listed along the left edge of the ZCB display. While on the **Backup** tab, you can create, edit, activate, deactivate, validate, delete, or clone backup sets by right-clicking a set. Then choose from the pop-up menu. The same operations are also available in the **File** menu in the user interface.

Activating/Deactivating a backup set: An Activated backup set will perform all its scheduled backups and be eligible for a restore operation. A Deactivated backup set will not perform scheduled backups, but will be eligible for a restore. You can re-activate a Deactivated backup set at any time, and the backup set will begin honoring the scheduled backups again. By default a backup set is in the activated state.

Validating a backup set: This is a simple way to check whether the essential configuration for the backup set is correct or not. If there are errors during validate, it indicates that the ZCB won't be able to use the configuration provided by the user to perform backup/restore operations correctly. Backup set configurations are automatically validated when configurations are saved as well as before any backup run is performed.

Deleting a backup set: Choosing the Delete Backup Set operation will present the user with the following two options. Select the correct option and press OK to continue with the deletion. Press CANCEL to abort the operation.

Delete this backup set configuration and all associated backup data from cloud and disk.

- Selecting this operation will remove the backup set from ZCB. Additionally, all data associated with the backup set, on both the local disk and on the cloud, will be deleted.
- A popup will appear to confirm the choice.

- This operation **cannot** be undone.

Just delete the configuration for this backup set from this computer, but retain the associated backup data.

- Selecting this operation will remove the backup set from ZCB, but all data will be left intact on both local disk and the cloud.
- A popup will appear to confirm the choice.
- The backup set can be recovered by running a Restore Catalog operation.

Cloning a backup set: This option will create an exact copy of the current backup set. Schedules can be carried over to the cloned backup set, or not, at the user's discretion. A cloned backup set can then be modified as necessary. Users who wish to create multiple, similar backup sets can use the clone feature to reduce setup time.

Configuring Backup Sets

ZCB makes it easy to configure backup sets by grouping the configuration options in four logical groups - **Backup What**, **Backup How**, **Backup Where** and **Backup When**.

Backup What

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

Backup Where

ZCB provides the flexibility of backing up to the cloud, to a local disk or a combination of both. It also allows retention periods to be configured separately for cloud and disk storages. This means that you have the flexibility to implement a disaster recovery strategy of your choice. You can use ZCB to perform the following backup solutions:

Backup to Cloud

This operation makes ZCB perform backups and transfer the backup data directly to the cloud. The backup data is not stored on the local disk. Generally, this operation is used when ZCB is the off-site backup solution while a separate solution is used for local backups.



The Backup to Cloud operation has limitations that may cause performance problems and/or backup failures. Please see [Info: Limitations of the Backup to Cloud operation](#).

Backup to Disk

This operation directs ZCB to perform backups and store them only on the local disk. The backup data is not uploaded to the cloud. Generally, this operation is used as the first step in a two-step approach to cloud backup where the data is first backed up to local disk and then uploaded at a later time, given the bandwidth and availability of other resources.

Please make sure that the local folder you select has enough available space. While calculating this space, please keep in mind the retention policy configured in the **Local Storage** option under the **Backup Where** section. Please refer to the [Retention Policies](#) section of this guide for more details.

Backup to both disk and cloud

This operation directs ZCB to first perform backup to disk and, upon its completion, immediately start uploading it to the cloud. The backup data is stored on the local disk as well as on the cloud. The backup set's Retention Policy governs how long the data is kept locally and in the cloud. Please refer to the Retention Policies section for more details.

Generally, this operation is used when a local copy of backup data is required for faster restores and extra redundancy. Cloud storage is used as the secure offsite data protection solution.

Please make sure that the local folder you select has enough available space.

Upload from disk to cloud

This operation directs ZCB to upload a backup stored on the disk to the cloud.

At times, business dictates that the best time to perform a backup is not necessarily the best time to perform an upload. The upload from disk to cloud function allows users to schedule backups at a different time than they are uploaded.

The most common use of this function is for backups scheduled throughout the day, which are later uploaded overnight.

Cloud Storage Options

Google stores your data in datacenters located across the world. You can choose from United States and Europe.

It is possible to have different cloud storage locations for different backup sets. However, please note that once configured, you can't change the cloud storage location for a backup set. If data for a single backup set were uploaded to multiple locations, it will be difficult for ZCB to perform restores.

Local Disk Storage Options

ZCB supports backing up to a local disk, an external hard disk or a network mapped drive.

Please see [How to use external or mapped network drives with ZCB](#).

Retention policies

A retention policy tells ZCB how long to retain backup data. When a backup run meets the age set in the Retention policy, it is purged.

While configuring the retention policy, consider the following:

- Your backup frequency and schedules (to ensure that older backups are not purged before a new backup is successfully created)
- Importance of older backup data (to ensure that you have access to older backup files even if they have been deleted or modified in newer backup runs)
- Free disk space and budget (to ensure that your backups don't fail due to lack of space or overshoot your defined budget)

ZCB allows you to specify retention policy separately for local and cloud storage.

Users may choose between two types of retention:

- **Number of successful full backups to retain:** Also known as time-based retention, this option allows users to keep a certain number of full backups plus all associated dependent backups.
- **Time period to retain backups for:** Also known as time-based retention, this option allows users to keep backups for a specific period of time.

Retention Policy Enforcement

When the retention policy is met, it is implemented by a Windows scheduled task with the name **Purge_ZIB_Backups**. This task is performed at midnight every day, but can be customized from the Preferences > Advanced menu. This task should not be removed from the Windows task scheduler. The purge schedule will run as soon as possible if it is unable to run at the scheduled time for any reason, including system shutdown.

Retention Policy Exceptions

If you choose time-based retention, ZCB offers two options to prevent deletion of backup data due to a misconfiguration of the retention policy. Both options are enabled by default, and we strongly recommend that they not be disabled.

Always Retain Last Full Backup: If this override is checked (default setting), the most recent Full Backup will not be purged even if it meets its retention period. This option ensures that you always have one Full backup to restore from.

Keep Backup If Dependent Backup Exists: If this override is checked (default setting), a backup will not be purged if another backup depends on it. This option ensures that you have all the data that is needed to perform a complete restore to any available backup point.

Changing Retention For Existing Backups

Changes made to time-based retention policies only apply to future backup runs. Existing backup runs are not changed automatically.

To change the Retention for old backups, please do the following:

1. Visit the REPORT page.
2. Select the backup you wish to change.
 - a. You may select multiple backups by CTRL+Click or SHIFT+Click.
3. Click the "Change retention period" icon or right-click.
4. Configure a new Retention Policy.
 - a. Options for "Local Retention Policy" will only appear for **Backups to Disk**. Likewise, "Cloud Retention Policy" will only appear for **Backups to Cloud** and **Uploads from Disk**.
 - b. Both options will appear for **Backups to Disk and Cloud** and if you select **multiple backups** of any sort.
 - c. You **cannot** change the Retention Policy of a "Purged" or "In Progress" backup.
 - d. You **can** change the Retention Policy for failed, canceled, successful, or paused backup
 - e. You **can** change the Retention Policy for backup runs retrieved via a Restore Catalog operation as well.

Bandwidth Throttling

By default, ZCB attempts to transfer data to and from the cloud at the maximum possible speed. Hence, ZCB always attempts to use the maximum bandwidth you have available.

If you wish to specify the maximum bandwidth (throttling) ZCB should use for upload and download of data, you can do so. Throttling can be set at a global level (affecting all backup sets) or configured for a specific backup set. For configuring these values globally, across all the backup sets, please go to **Preferences > Bandwidth**. For configuring these limits at a backup set level, so that they override the global values, please go to **Cloud Storage** sub-section in the **Backup Where** section.

ZCB allows you to configure bandwidth throttling in these two ways:

Uniform Throttling:

If you wish to configure uniform throttling values, irrespective of the time of the day and day of the week, then you can simply configure these two options:

Max Upload Rate: This value, in kilobits per second, refers to the maximum bandwidth ZCB will use for uploading backup data to the cloud.

Max Download Rate: This value, in kilobits per second, refers to the maximum bandwidth ZCB will use for downloading backup data from the cloud.

Time-based Throttling:

If you want ZCB to use different throttling values during different hours and different days of the week, then you can configure time based bandwidth throttling. To configure this, click on the **Throttle by Time** button for upload or download. The resulting pop up window will show the days of the week and different time slots in each day. Each time slot is of 15 minutes in duration.

To begin configuration, you can select the cells from the time table shown and input the desired value in the **Maximum Rate (kbps)** box. Click on **Apply Custom Rate to Selected Slots** to apply the provided value to the selected slots. Please note that configured values take effect only for future data transfers. Any ongoing jobs will continue to use any previously configured values ("unlimited" by default).

For ease of use, ZCB comes with predefined templates for time based bandwidth throttling. You can choose a template from the **Choose Predefined Template** dropdown. If you wish to tweak the template values, you can select the time slots as described above and configure different values.

Secure Transfer (SSL)

ZCB automatically provides secure transfer of data to cloud using the Secure Socket Layer (SSL) protocol.

Backup How

ZCB supports compression and encryption of user data. Data is compressed and/or encrypted during the backup process. It is written to disk or uploaded to cloud only after the encryption/compression is completed. This ensures that, at no point, will the backup data be unencrypted.

The user can specify the following settings:

Compression

This can help save network bandwidth and reduce the storage space required for backups. Compression level can range from Off (no compression) to Max (maximum compression). The actual compression ratio depends on the type of your data. Files such .txt and .doc compress well, while media files such as .mp3 and .jpg do not.

Note that higher levels of compression are CPU intensive and may impact system performance. If high compression is desired, scheduling the backup during non-peak hours may be desirable.

Encryption

ZCB offers two different types of encryption:

- Auto Encryption (Available for ZCB with Google Cloud Storage *only*)
- Private Key Encryption (Available for both ZCB with Google Cloud Storage and ZCB with Amazon S3)

Auto Encryption

ZCB with Google Cloud Storage will automatically encrypt your backups on the cloud.

Transfer of your backup data to the cloud is secure using the Secure Sockets Layer (SSL) protocol. The encryption itself takes place server-side on the cloud.

Auto Encryption is not available in ZCB with Amazon S3.



Auto Encryption only applies to backups stored on the cloud. Local backups will not be encrypted. If encryption of locally-stored backups is required, you must use the Private Key Encryption option.

Private Key Encryption

With Private Key Encryption, each user will create a unique encryption key generated from a passphrase. The encryption key or passphrase is *required* in order to restore data.

Private Encryption Keys will encrypt your backups using AES-256 bit encryption. AES-256 bit encryption is trusted worldwide.



If Private Key Encryption is chosen, *you* are responsible for safe and secure storage of your encryption keys. Zmanda does not store your encryption keys or passphrase anywhere.

Replacement keys can be created if you remember your chosen passphrase.

If you lose your private encryption key *and* forget your passphrase, neither you nor Zmanda will be able to decrypt your encrypted backup data.

Create a new Private Encryption Key

You need to first create a personal encryption key. To create the key:

1. Click on **Add Private Encryption Key** in Backup How.
2. A new window will appear.
3. Enter a **Key Name**.
4. Create a passphrase.
 - a. The passphrase must be at least four characters in length.
 - b. By default, ZCB will save this newly created key in ZCB's Encryption folder, but you may choose an alternate location.
5. Click **OK**.
6. A new window will appear to confirm that the encryption key was created.
7. Click **OK**.
8. Save the backup set/
9. All future backups for this backup set, local and cloud, will be encrypted using your Private Encryption Key.

Select an existing Private Encryption Key

You may use an already-existing Private Encryption Key with other backup sets.

1. Click on the backup set on the left side panel.
2. Click on **Add Private Encryption Key** in Backup How.
3. A new window will appear and ask you if you wish to use the existing key.
4. Click **Enable**.
5. Save the backup set.
6. All future backups for this backup set, local and cloud, will be encrypted using your Private Encryption Key.

Delete or Modify an existing Private Encryption Key

To delete an encryption key:

1. Select any backup set for which Private Key Encryption is enabled.
2. Click the **Delete Key** link found in Backup How.
3. A window will appear to confirm your deletion and warn that a copy of the key should be kept for decryption purposes.

Existing Private Encryption Keys cannot be modified. To change a key, first delete a key and create a new one.

Backup When

Pre-backup and Post-backup Actions

ZCB offers the flexibility of running custom commands or scripts before it begins a backup or after it finishes a backup. For instance, if one wishes to copy certain files from outside the backup directory to inside just before backup is run, he/she can configure a pre-backup action. Similarly, if one wants to invoke another program (such as an old data purging script) after backup is completed, a post backup action can be configured.

To configure these actions, please select the backup set from the left hand pane and go to the **Backup** tab. In the **Backup When** section, under the **Backup Set Preferences** tab, you can locate this setting. Please browse for the batch script or other executable program present on your machine that you want ZCB to execute before/after the backup. Then save the backup set configuration.

Please note the following important points:

- If you want to add parameters to the above script or program, then please click on the Pre-backup/Post-backup icon again and add the parameters to the command that is shown by ZCB.
- If the configured Pre-backup or Post-backup actions fail upon being run by ZCB, the backup is marked as failed. The exit status of the failed command can be found in the ZCB log file. If you wish to make ZCB continue with the backup, despite any error in running the command, you can do so by making your script exit with a special exit status of 65531.

- If your script is opening files for reading/writing, make sure that file names are fully qualified file names (e.g. C:\backup\Log.txt). Unqualified names such as "Log.txt" will result in files getting created inside C:\Windows\system32 folder.

Email Notification

You can configure email notifications to be sent when each operation completes. You can customize the notification settings at the backup set level.



Email notifications cannot be configured until the SMTP server information is correctly configured in the Preferences > Emails menu. Please refer to the [Email Notification](#) section for more details.

Scheduling

ZCB offers powerful and completely flexible scheduling options. You can schedule each of the following operations independently– **Backup to cloud**, **Backup to disk**, **Backup to both disk and cloud** and **Upload backup data from disk** at your desired time. For example, this gives you the flexibility to schedule **Backup to disk** operations on weekdays and **Upload backup data from disk** operation on weekends when your bandwidth is not in high demand.

To add scheduled backup runs for a backup set, please select the backup set from the left hand pane and go to the **Backup** tab. In the **Backup When** section, under the **Scheduling and Retention** tab, click on the **Schedule Templates** button. This will show you many schedule templates to choose from. Each template is completely customizable. Don't forget to click the **Save Backup Set** button at the bottom of the Backup page to commit the schedule.

Schedules follow the rules for Microsoft Task Scheduler, as outlined in the following document. Different versions of Windows may handle overlapping schedules differently. For details, please refer to this Microsoft Technet article: [http://technet.microsoft.com/en-us/library/cc722178\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc722178(v=ws.10).aspx)

ZCB can also be set to wake the PC to run the backup if the PC is in Sleep, Standby, or Hibernate mode. The **Wake the system to run this task** option is enabled by default. However, the wake function behaves differently from one version of Windows to another.

On Windows XP

- In Hibernate Mode:
 - If wake is enabled, the PC **will not** wake. The backup will start automatically when the machine is awakened by the user.
 - If wake is disabled, the backup will be skipped entirely.
- In Standby Mode:
 - If wake is enabled, the PC will wake and the begin the backup.
 - If wake is disabled, the backup will be skipped entirely.

On Windows Vista

- In Sleep Mode:
 - If wake is enabled, the PC will wake and the begin the backup.
 - If wake is disabled, the backup will be skipped entirely.

On Windows 7 and Windows 8

- First, the Allow Wake Timers setting must be enabled.
 - Go to the Control Panel > All Items > Power Options > Edit Plan Settings.
 - Select Change Advanced Power Settings. Go to the Sleep Tab.
 - Enable Allow Wake Timers.
- Sleep and Hibernate Modes behave the same.
 - If wake is enabled, the PC will wake and begin the backup.
 - If wake is disabled, the PC will begin the backup when the machine is awakened by the user.

Performing Backups

Once you have saved the backup set, you can perform backups. You can either launch a manual backup or add schedules to backup automatically at a specific time.

To run a manual backup, select the backup set from the left hand pane and go to **Backup** page. In the **Backup When** section, under the **Backup Now** tab, choose the operation which you want to run and click on the button just below it to launch the selected operation. To configure scheduled backup runs, please see the [Scheduling](#) section.

Below is detailed information for all applications you can backup using ZCB.

For all backups involving mapped network drives, please see [How to use external or mapped network drives with ZCB](#).



Backups of databases, including Microsoft SQL Server, Exchange, and Sharepoint, must only be backed up by one backup application. If more than one application is backing up a database, Differential and/or Incremental backups will fail. This is a limitation of the

database software itself, not of the backup application(s) in question.

Therefore, it is recommended that you turn off any other backup programs when you first configure ZCB.

For more information, please see [Info: How do databases handle backups from multiple different backup applications?](#)

Windows File System

Overview: ZCB can perform full (all files), differential (only files which changed since last full backup) and incremental (only files which changed since any last successful backup) backups of Windows NTFS and ReFS file systems. It can backup open files and doesn't have any limit on the size of the files to be backed up. In addition, it can also backup files from an external portable hard drive or a network mapped drive.

Functionality: When backing up an NTFS or ReFS file system, ZCB lets you select directories and files from a browser tree.

You can specify the list of files to be excluded during a Windows file system backup. Windows file systems support wild cards in the exclude specification. Wild cards "" (match one or more characters) and "?" (match exactly one character) are supported. The pathname in the exclude specification must be the 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".

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

Requirements:

- Windows NTFS and ReFS file systems are supported.
- For backing up open files, the Volume Shadow Copy Service must be enabled.
- If your backup set includes files from encrypted volumes, or files that individually have encryption enabled, consider backing up the associated encryption keys so that you can access the files after restoring them with ZCB.

A note about Network Mapped Drives:

You can use ZCB to back up the data on network drive. You may also choose it as your local storage for keeping your local backup archives. Please see [How to use external or mapped network drives with ZCB](#).

Requirements for Backups of a Distributed File System

ZCB can be used to backup and restore folders that participate in DFS replication topology, with the following exception:

ZCB must be installed on the host where replicated the DFS share is configured. ZCB relies on the DFSR VSS Writer for correct functionality of backup and restore operation.

Backup and restore of a network shared folder which is a member of a DFS replication group is not supported.

Junction Point directories in Windows Vista and onwards will not be backed up. Please make sure that the source directory is included in your backup set. More information can be found in [Warning: Files under junction point directories are not backed up](#).

Microsoft SQL server

Overview: Users can perform VDI-based backups of a specific database on a specific SQL server instance. Full, Differential, and Incremental (Log) backups are supported.

To configure MS SQL server backups, create a new backup set and choose **SQL Server** from the dropdown list in the **Backup What** section. ZCB will discover all SQL Server components and will display them in the Backup What section in the following format:

```
MSSQL-2008\Servername\InstanceName\DatabaseName  
MSSQL-2005\Servername\InstanceName\DatabaseName  
MSSQL-2000\Servername\InstanceName\DatabaseName
```

From this list, you can select the ones which you wish to back up and save the backup set.

Functionality: ZCB supports Simple Recovery Model, Full Recovery Model and Bulk Recovery Model for SQL server databases.

- **Simple Recovery Model**
 - The full backup will contain .MDF, .LDF and .NDF (in case of filegroups) files in the backup image.
 - The differential backup will contain .LDF files.
 - Incremental (Log) backups will be skipped for databases using the Simple Recovery Model
- **Full Recovery Model**
 - The full backup will contain .MDF, .LDF and .NDF (in case of filegroups) files in the backup image.
 - The differential backup will contain the changed blocks of the .MDF database file.
 - Incremental (Log) backups will contain .TRN files (transaction logs flushed to the disk). These are transactions that have changed since the last backup of any level, be it Full, Differential, or Incremental.
- **Bulk Recovery Model**
 - The full backup will contain .MDF, .LDF and .NDF (in case of filegroups) files in the backup image.
 - The differential backup will contain the changed blocks of the .MDF database file.
 - Incremental (Log) backups will contain .TRN files (transaction logs flushed to the disk). These are transactions that have

changed since the last backup of any level, be it Full, Differential, or Incremental.

Please note the following:

- The master and model databases are only backed up as part of the full backups. During restore of master database, SQL server is stopped and is restarted after restoration.
- Any read-only databases are only backed up as part of the full backups.
- ZCB will only back up MS SQL databases that are in the Mounted state.
- A backup set created to backup MS SQL 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 File System backup set to back up the other crucial MS SQL files.
- Please note that SQL server backup set validation checks for **amandabackup** SQL user but does not check if the privileges are sufficient for backup and recovery.

Requirements:

- The Windows **amandabackup** user must be added as a SQL server user with sufficient privileges. Please see [Allowing access to Microsoft SQL Server](#)
- The Volume Shadow Copy Service must be enabled. This means that its startup type must be either automatic or manual. Please refer to the [Requirements](#) section for how to do this.
- Microsoft recommends that MS SQL and System State backups should not be run simultaneously.
- The SQL VSS Writer service must be running at the time of backup and recovery. ZCB will automatically start the SQL Writer service.
- Please ensure that you have enabled TCP/IP on your MSSQL server. You can do this using the "SQL Server Configuration Manager" tool.



If you set up both Microsoft SQL backups and Sharepoint backups, be sure to remove all Sharepoint databases from your Microsoft SQL Server backup set. Failures may occur if the same database is being backed up by two different methods.

Microsoft Exchange Server

Overview: ZCB supports full, incremental and differential backups of Microsoft Exchange Mailbox Databases and Public Folder Databases. To configure Microsoft Exchange server backups, create a new backup set and choose **Exchange** from the dropdown list in the **Backup What** section. ZCB will discover all Exchange Server components (such as Mailbox) and will display them in the Backup What section in the following format:

MSExchange-2013\Servername\MailboxStoreName\File
MSExchange-2013\Servername\MailboxStoreName\Logs

MSExchange-2010\Servername\MailboxStoreName\File
MSExchange-2010\Servername\MailboxStoreName\Logs
MSExchange-2010\Servername\PublicFolderStoreName\File
MSExchange-2010\Servername\PublicFolderStoreName\Logs

MSExchange-2007\Servername\StorageGroupName\MailboxStoreName
MSExchange-2007\Servername\StorageGroupName\PublicFolderStoreName
MSExchange-2007\Servername\StorageGroupName\Logs

MSExchange-2003\Servername\StorageGroupName\MailboxStoreName
MSExchange-2003\Servername\StorageGroupName\PublicFolderStoreName
MSExchange-2003\Servername\StorageGroupName\Logs

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

Full Backups contain the Mailbox database (.edb & .stm files), transaction logs, and checkpoint files. After a successful Full Backup, Exchange will purge all committed transaction logs. An event is logged in the Windows Application Event Logs.

Incremental Backups contain the transaction logs only. After a successful Incremental backup, Exchange will purge all committed transaction logs. An event is logged in the Windows Application Event Logs.

Differential Backups contain the transaction logs only. No logs are truncated after a successful Differential backup.

Requirements:

- Exchange backups have additional dependencies, as noted in System Requirements.
 - Upon creation of an Exchange backup set, a popup will appear if one or more dependencies are not installed on the system.
 - The **Check Dependencies** option in the **Tools** menu may also be used to check for Exchange backup dependencies.
- 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.
- In Windows 2003 Small Business Server edition, the Exchange Writer is **disabled** by default.
 - ZCB will attempt to enable the VSS writer for you. However a manual restart of the Microsoft Exchange Information Store service will be required.

- If ZCB cannot enable the VSS Writer, please follow the instructions in this Microsoft knowledgebase article to enable the Exchange Writer: <http://support.microsoft.com/kb/838183>
- 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 **Microsoft Exchange Information Store** Service.
- Latest Exchange service pack must be installed. For example: Exchange 2003 Server Service Pack 2 or later must be installed.
- Make sure that the Exchange Storage Groups are in Mounted state.
- The **Windows Management Framework** must be installed on the system.
- The **amandabackup user** is automatically assigned to the View Only Organization Management role in the Exchange Security Groups
 - If the amandabackup user must be added to the Exchange Security Groups manually, follow these steps:
 - Open "Active Directory Users and Computers"
 - For Exchange 2007: Add the amandabackup user to Microsoft Exchange Security Groups > View Only Organization Management
 - For Exchange 2010 and 2013: Add the amandabackup user to Microsoft Exchange Security Groups > Exchange View-Only Administrators
 - The Zmanda Cloud Backup Services must be restarted after *amandabackup* is added to the Exchange Security Groups
 - Click on Tools > Restart Services in the ZCB User Interface, or restart ZCBService and ZWCService manually from the Windows Services Panel
- Exchange circular logging must be disabled. In most cases, you **will not** need to disable Circular logging manually, as ZCB will do it for you.
 - Circular logging allows Microsoft Exchange to overwrite transaction log files after the data that the log files contain has been committed to the database. By enabling circular logging, you reduce drive storage space requirements. However, without a complete set of transaction log files, you cannot recover any data more recent than the last full backup. Differential and Incremental backups will fail.
 - Therefore, in a normal production environment, circular logging is not recommended.
 - For instructions on how to disable circular logging, please follow Microsoft articles below:
 - **Exchange Server 2007, 2010:** <http://technet.microsoft.com/en-us/library/bb331968%28v=exchg.80%29.aspx>
 - **Exchange Server 2003:** <http://support.microsoft.com/kb/314605>

Microsoft SharePoint

Overview:

ZCB supports back up of Microsoft SharePoint in standalone and single-server farm configuration. Backups of multi-server Sharepoint farm configurations are not supported.

To configure Microsoft SharePoint server backups, create a new backup set and choose **SharePoint** from the dropdown list in the **Backup What** section. ZCB backs up SharePoint data that is stored in the SQL database & application web site files, such as:

- Configuration and Admin databases
- Content and configuration data for Web Applications (Eg: C:\Program Files\Microsoft Office Servers\14.0\Data\Office Server\Applications)
- Any third-party databases that are registered with SharePoint
- Shared services databases in SharePoint
- Office Search & Help Search index files

Functionality:

- ZCB performs full & differential backups of the SharePoint data based on the modification time.
- ZCB does not support transaction log 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.
 - Files, documents, the folders that contain them, and the Sharepoint installation directory itself should be backed up as part of a separate File System backup.
 - IIS metabase information, ports, host header, authentication, and other such configuration data is included as part of a System State backup.
 - Please see [this blog post](#) for more information on the relationship between Sharepoint and the IIS metabase.
- 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:

- 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. Please refer to the [Requirements](#) section.
- The SQL VSS Writer service must be running at the time of backup and recovery. ZCB will automatically start the SQL VSS Writer service.
- The Windows SharePoint Services VSS Writer service will be registered and started automatically by ZCB.
- The SharePoint VSS writer depends on other VSS writers, such as OSearch and SPSearch. These writers must be enabled and set to automatic start for Sharepoint backups to function.
 - For Sharepoint 2010
 - SPSearch4 VSS Writer
 - Enable by starting the *SharePoint Foundation Search V4* service.
 - OSearch14 VSS Writer

- Enable by starting the *SharePoint Server Search 14* service.
- For SharePoint 2007
 - OSearch VSS Writer
 - Enable by starting the *Office SharePoint Server Search* service.
 - SPSearch VSS Writer
 - Enable by starting the *Windows SharePoint Services Search* service.
- 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.



Special Requirement for WSS 3.0

The default installation of Windows SharePoint Services 3 instances will use the Windows Internal Database (MICROSOFT##SSEE), which is run under the "Network Service" system account.

In such a case, the "Network Service" account must have Full Control permissions to the Zmanda Cloud Backup "misc" directory.

By default, the misc directory is located here:

- For Windows Server 2003: C:\Program Files\Zmanda\Zmanda Cloud Backup\misc\
- For Windows Server 2008 and 2012: C:\ProgramData\Zmanda\Zmanda Cloud Backup\misc\

Windows System State

Overview:

Windows System State refers to a collection of several key operating system elements and their files. Backing up the Windows System State is crucial for a successful disaster recovery strategy. ZCB can back up the Windows System State of all supported Windows platforms.

Windows System State is always a full backup.

Contents of a Windows System State Backup:

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

- **Boot Files:**
 - For Windows versions older than Vista: **SystemDrive\NTDETECT.COM**, **SystemDrive\ntldr**, **SystemDrive\boot.ini** (**SystemDrive** is usually **c:**).
 - On Windows Vista and newer: **SystemRoot\boot** directory (**SystemRoot** is usually **c:\windows**)
- **Catalog files:** **SystemRoot\System32\CatRoot**.
- **MachineKeys Files:** **SystemRoot\System32\Microsoft\Protect*** and **AllUsersProfile\ApplicationData\Microsoft\Crypto\RSA\MachineKeys*** where **ALLUserProfile** is **c:\Documents and Settings\All Users**.
- **Performance counters:** perf*.dat and perf*.bak files in **c:\windows\system32** on all Windows versions.
- **WFP files:** All dll and exe files that come under Windows File Protection (WFP). Usually the dll files reside in **c:\windows\system32**
- **IIS metadata** file if IIS is installed (applicable to all Windows versions).
- **Certificate Database** (Applicable to only Windows 2003 server that are Certificate Servers): files in **c:\windows\system32\certsrv**
- **COM+** registration database.
- **Registry:** System, default, SAM, Security and Software files in **SystemRoot\system32\config** and additional Components and Schema files in Vista.
- **Active Directory:** If Active Directory is installed, backups include the database, log files, and Group Policy Objects (GPOs).

Requirements:

- Please check the operating system and service pack requirements as mentioned in the [Requirements](#) section.
- The Volume Shadow Copy Service must be enabled. Please refer to the [Requirements](#) section.
- System state backups of a Windows Domain controller that holds the Active Directory Certificate Services role may encounter a "System state writer missing" error. Refer to [this Microsoft Knowledgebase article](#) to resolve the problem.
- System State backups should not be run at the same time as Microsoft SQL Server backups.

MySQL Server

Overview:

ZCB supports logical backup of MySQL Server version 5.x.

To configure MySQL server backups, create a new backup set and choose **MySQL Server** from the dropdown list in the **Backup What** section. Here, please specify the MySQL server information and user credentials of the user that can perform the backup. MySQL client path refers to the directory where the MySQL client utilities compatible with your MySQL server are present.

ZCB assumes the following defaults. Please change them if necessary.

- **MySQL Server:** localhost
- **Port:** 3306



If your MySQL instance uses a socket file for connection instead of a port, please leave the Port field blank.

After filling in the details, click on the **Discover** button so that ZCB can connect to the MySQL server and read the databases and tables present in it.

Functionality:

- Only full backups of MySQL servers are supported currently. ZCB doesn't backup MySQL binary logs.
- ZCB supports backup of specific MySQL databases.
- ZCB supports backup of specific tables only from one MySQL database. It does not support selecting specific tables from multiple MySQL databases.
- You can either backup a local MySQL server or a remote MySQL server.

Requirements:

- The amandabackup user should have sufficient privileges to perform logical backup from the ZCB machine. The minimal set of privileges required are:

For backup:

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

For 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.

Oracle Server

Overview:

ZCB supports backup of Windows Oracle 11i.

To configure Oracle server backups, create a new backup set and choose **Oracle** from the dropdown list in the **Backup What** section.

Functionality:

- ZCB supports Full, Differential and Incremental backups of Oracle databases.
- The Oracle components that are backed up by ZCB are Oracle database, Control File, Server Parameter file, All table spaces and Archived logs. All backup files & archived logs from the Flash Recovery Area are also included in the snapshot. The online redo logs will not be included in the snapshot.
- ZCB does not support selective backup of individual databases, log files, control files, etc.

Requirements:

- The Oracle VSS Writer service must be installed for the Oracle instances that need to be backed up. The Oracle VSS Writer service must be in Started & Automatic state. In case the Oracle VSS Writer service is not installed by default, please refer to the Oracle documentation to install the service [Installing and Uninstalling the Oracle VSS Write Service](#).
- 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. Please refer to the [Requirements](#) section.
- All Oracle databases in **NOARCHIVELOG** mode must be **Mounted** and in **Read-Only** state. The database cannot be **Open** in **Read Write** mode, else the backup will fail.
 - A backup may contain multiple databases. If one database is in **Read-Only** state and the others are in **Read-Write** state, the backup for all databases will fail.
- Oracle database in **ARCHIVELOG** mode may be **Open** in **Read Write** or in **Mounted** state.

Hyper-V

Overview: ZCB supports backup and restore of virtual machines hosted by Hyper-V server installations. Servers in "core" configuration are not supported.

To configure Hyper-V server backups, create a new backup set and choose **Hyper-V** from the dropdown list in the **Backup What** section. The host configuration and any configured VMs will be automatically detected.

Functionality:

Hyper-V backups are always **Full Backups**. Backups are taken using the Hyper-V VSS Writer.

Users may select individual virtual machines within the Hyper-V host for backup. This will backup the virtual hard disk files (.vhd or .vhdx) as well as the snapshot files (.avhdx or .avhdx) of the virtual machine(s) selected for backup.

Backup of the Initial Store is also available. This will backup the "InitialStore.xml" file, which contains the Hyper-V Authorization Store. By default,

the InitialStore.xml file is in %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V.

Hyper-V uses one of two mechanisms to back up each VM. The default backup mechanism is called the "Saved State" method, where the VM is put into a saved state during the processing of the PrepareForSnapshot event, snapshots are taken of the appropriate volumes, and the VM is returned to the previous state during the processing of the PostSnapshot event.

The other backup mechanism is called the "Child VM Snapshot" method, which uses VSS inside the child VM to participate in the backup. For the "Child VM Snapshot" method to be supported, all of the following conditions must be met:

- Backup (volume snapshot) Integration Service is installed and running in the child VM. The service name is "Hyper-V Volume Shadow Copy Requestor".
- The child VM must be in the running state.
- The Snapshot File Location for the VM is set to be the same volume in the host operating system as the VHD files for the VM.
- All volumes in the child VM are basic disks and there are no dynamic disks.
- All disks in the child VM must use a file system that supports snapshots (for example, NTFS).

You can read more about Hyper-V backups here: <http://msdn.microsoft.com/en-us/library/dd405549%28v=vs.85%29.aspx>

Back up a running VM only if its hot backup can be performed is a special option designed to keep VMs running smoothly during backup. If enabled, ZCB will skip backup of a running VM when the "Child VM Snapshot" method cannot be performed.

Monitoring

The **Monitor** page displays the status of backups, restores, uploads and downloads operations in progress for all backup sets. Please note that Monitor page shows only the most recent in-progress task for a backup set.

Different operations can be clicked or right-clicked to display different options. For instance, you may want to stop any ongoing task, or may want to pause an upload operation to reduce network bandwidth usage during peak office hours.

The summary of available options for each type of operation is below.

Operation Option	Stop	Pause	Resume
Backup to Cloud	Yes	Yes	Yes
Backup to Disk	Yes	No	No
Upload to Cloud	Yes	Yes	Yes
Download	Yes	No	No
Restore	Yes	No	No

Please note that if you are resuming an upload job, ZCB will also resume any incomplete upload jobs pending for that backup set. If you wish to resume only one job, please use the **Report** page.

Upload speeds are shown on the Monitor page only. The current speed and the average speed are displayed in the details column.

Reporting

The **Report** page displays a table of various historic operations performed by ZCB.

Report History

A history of all operations will be displayed on the Report Page. Each line references a specific operation and contains many details about the operation.

- A green checkmark icon indicates the operation was successful.
- A red X icon indicates the operation failed. Please see the Details column for more information.
- A yellow warning icon indicates a warning. The backup was successful, but please reference the Details column for more information.



If a blue info icon is present in the details column, the icon can be clicked to obtain further information.

Manage Report History

You can click on any column heading to sort by that field. Columns can be dragged to display in any order.

By default, the history is kept forever. The length of the history can be customized from the **Preferences > Advanced** menu.

Report Templates

ZCB allows you to customize your historical view. Please click on **Define Template** button, specify the template name and choose the columns which you want to include the template view. Click on Save Template to add this new template.

To load a specific template, you can select it from the dropdown just next to the **Define Template** button.

To export your loaded template view to a Comma Separated Values (CSV) file, please click on the **Export Report** button. This file can be used for printing, or import into other applications to create spreadsheets and charts.

Verify Backup Data

If you have recently moved or deleted backup files from local disk or the cloud, you may want to verify that ZCB can access your backup data correctly.

You may verify your data by selecting a backup run and clicking the Verify Backup Data icon or by right-clicking and choosing Verify Backup Data. The verification process will return a Success, Warning, or Fail status along with a brief explanation for all Failures and Warnings.



This operation only checks for the existence of the backup data. It doesn't check the integrity of backup data.

Also, operation cannot be initiated for In-Progress, Paused or Purged backups or uploads. It is also not available for Backup to Cloud operations that are marked as Failed or Canceled.

Task Management

Select the task you wish to modify. Once selected, you may right-click to bring up a menu or click the icon at the top of the page that corresponds to the action you wish to perform.

Here is a summary of what actions are allowed on what type of jobs.

Job Action	Delete Backup Run	Delete Data from Disk	Delete Data from Cloud	Begin Upload
Backup to Cloud	Yes	No	Yes	No
Backup to Disk	Yes	Yes	No	Yes*
Upload from Disk	Yes	No	Yes	No
Download	Yes	No	No	No
Restore**	Yes	No	No	No

*Available only if data from disk is not uploaded.

**Options will say "Restore" instead of "Backup".

Please note that if you select multiple tasks the only action available is "Delete Backup Run".

ZCB Global Dashboard

In addition to the Report page, backups on the cloud can be monitored using the [ZCB Global Dashboard](#). This powerful, web-based tool shows detailed reports on all current cloud backups for all machines under your account. For more information, visit our [website](#).

You can launch the ZCB Global Dashboard by clicking the "Monitor using the ZCB Global Dashboard" link found at the top of the Report page. You can also access the dashboard by visiting <http://zgd.zmanda.com> from any web browser.

Log in to the ZCB Global Dashboard with your existing Zmanda Network credentials.

Restore

ZCB offers a number of ways to restore file system and application backups. You can restore to the original backed up system or a different system altogether.

Overview

What is a Backup Catalog?

When ZCB backs up data, it stores some key meta-information in a special file called the backup catalog. This catalog is used by ZCB at restoration time to let the user select the desired specific data for restoration and to restore the backup data correctly.

Restore to the original machine

This is the most common case where one wishes to restore data to the same machine where it was backed up. To do this, you need to go to **Restore** page and follow the below-mentioned instructions as applicable for the type of backup data you wish to restore.

Restore to a different machine

You can also restore backup data originating from one machine to a different machine. This is mostly used to create a clone of the original system as done in a bare-metal recovery scenario. Doing this requires some additional steps before you can launch the actual restore process. The steps are:

- It is recommended that you install the same Windows Operating System (with the same service packs) on the restore machine as was installed on the original machine.
 - This is required for System State backups
- For *all* Microsoft Exchange, Microsoft Sharepoint, and Hyper-V backups, the name of the new machine must exactly match the name of the old machine.
 - For Exchange, the recovery server must have the same Organization name, same Storage Group name, and same Mailbox or Public Folder database name as the original server.
 - For Sharepoint, the instance name must match the name from the original server.
- For Microsoft SQL Server, the instance name must exactly match the names from the original server.
- Install ZCB on the target machine (where you wish to restore the backup data).
- Import cloud certificate as described in section above.
- Complete the process of restoring the catalogue as described in the section [Restoring the Backup Catalog](#).
- Once the backup catalog has been downloaded by ZCB successfully, you can follow the normal restoration steps as explained in the [Performing Restores](#) section as applicable for the type of backup data you wish to restore.
- The *amandabackup* user must have full access to the folder where the backups are stored.
 - For cloud backups, this is the folder to which you download the backup.
 - For local backups, this is the folder where the backup is stored.
- Likewise, the *amandabackup* user must have full access to the directories to which the backups are being restored.

Restore Options

Run Script Before Restore: This optional field lets you specify an executable file (example .bat and .exe) which you want to run just before the actual restore is performed.

Run Script After Restore: This optional field lets you specify an executable file (example .bat and .exe) which you want to run just after the actual restore is performed.

Download Folder: This path refers to the location where ZCB should download the backup archives from the cloud.

Restore Folder: This optional field is required if you wish to restore the selected files and folders to an alternate location and have selected the Alternate Location radio button just below this field.

Restore to Alternate Location: If selected, this radio button directs ZCB to write restore data to a location as defined in the Restore Folder field above.

Restore to Original Location: If selected, this radio button directs ZCB to write restore data to the original location. If this is chosen, you would want to carefully choose the correct conflict resolution option in the Restore Policy dropdown just next to this field.

Restore Policy: ZCB offers 4 conflict resolution options if it encounters a file already present in the folder where restore data is being written. These options are:

Keep Existing: This will make ZCB retain the already present file and skip the restore for it.

Overwrite Existing: This will make ZCB overwrite the already present file with the version contained in the restore data.

Rename Existing: This will make ZCB rename the already present file with a timestamp suffix appended to its original name. The file contained in the restore data will be restored with its name being intact.

Rename Restored: This will make ZCB retain the already present file and the file contained in the restore data will be restored with a timestamp suffix appended to its original name.

Retain Download Archive: By default, once the restore is complete, ZCB will delete the backup archive downloaded from the cloud. If you wish to retain this archive so that you can do more restores from this backup run later, you can select this option. Please note that you will have to manually delete the downloaded archive when you no longer need it.

Skip Archive Verification: ZCB performs an archive consistency check on the backup archives prior to restore. Archive verification can

take a long time. Checking this box disables the archive verification for **local backups** only. Archive verification cannot be disabled for cloud backups.

Advanced Filtering

To filter items, users may specify patterns that include wildcards, combine them with 'and' or 'or', as well as apply negation to the whole pattern. The syntax for the pattern expressions is as follows:

- "Or" filtering = pattern||pattern
- "And" filtering = pattern&&pattern
- "Not" filtering = !pattern
- The pattern may contain any **alphanumeric characters, path separators** (only backward slashes), or **any characters that are valid in a file path name**
- ZCB automatically searches for any result that includes the submitted string.
 - For example, if the word **test** is submitted, all files and directories that contain **test** will be returned.
 - If the submitted string contains an asterisk *, the asterisk will be used as a wildcard.
 - If no wildcards are used, any result that matches the string will be returned.
- Absolute paths can be specified as follows: **C:\Users\FileServer*.txt** or **C:\Users\FileServer**.

Examples of OR:

- **jpg|txt|docx** to show either jpg, txt, or docx files.
- **C:\Users\FileServer*.txt|.docx** to show any .txt files in C:\Users\FileServer **or** any .docx files in any directory.

Examples of AND:

- **C:\Users&&jpg** to show all jpg files in the C:\Users directory.
- **Products&&TestData** to show all files that are both in the Products directory and the TestData directory.

Examples of NOT:

- **!pdf** to show all files that are not pdf.
- **!Users** to show all files that are not in the Users directory.

Examples of EXACT:

- **"C:\Users"** to show the C:\Users\ directory.
- **"MSSQL-2005:WINDEV-REPLACE\MSSQLSERVER\A1"** to show the MSSQL-2005:WINDEV-REPLACE\MSSQLSERVER\A1 database.

Restore the Windows File System

Overview: For Windows File System restores, ZCB offers a lot of finer options to allow the user to have just the right control and flexibility while restoring the data. You can restore to the original backed up system or a different system altogether.

Functionality:

To perform restore of file system data, please follow the following steps:

- In the ZCB user interface, select the backup set for which backup was taken and please navigate to the Restore page and from the table showing all the backup runs, click on the run which you want to use for restore.
- In the Restore Point dropdown, ZCB will show you all the relevant backup images for this restore operation. The restored data will be exactly same as it existed at the time stamp contained in the backup run images.
- Once you select a restore point, all the files which are available for restore will be shown.
- ZCB lets you select directories and files from a browser tree. You can use the Filter option to search specific files/folders. ZCB supports wild cards in the Filter specification. Wild cards "" **(match one or more character)** and "?" **(match exactly one character)** are supported. **You can either enter absolute path of the files to be searched. In case you do not remember the absolute path, use "*Filename" pattern.** Example, to search all files with .jpg extension, enter ".jpg". **To search all files under "C:\Windows\System32", enter "C:\Windows\System32" or "*System32" as the search pattern.**



Note about restoring NTFS files to ReFS drives

Some NTFS features are not supported by the ReFS file system. NTFS files and folders can only be restored to ReFS file systems if their properties are compatible.

Files with the following attributes are not supported by ReFS, and therefore will be skipped at the time of restore.

- Named Streams
- Object IDs
- 8.3 Filenames
- NTFS Compression
- Encrypting File System (EFS)

- Transaction NTFS
- Hard links
- Extended Attributes
- Disk Quotas

Locate A Backed Up File

This option allows you to search for a file **across all backup runs** for a backup set and restore its latest version quickly. This can be useful when you have a lot of backup runs and don't remember which backup run contains the file you need.

After clicking the **Locate A Backed Up File** button, simply enter as much of the file name or the file path as you remember. ZCB will search for this in all the backup runs and return a list of all files and directories that contain the name you entered and the most recent time they were backed up.

You can select the file from this result window and click on the "Select this file for Restore" button. Then provide your restore preferences in the main Restore page, and hit Restore button to restore the latest version of this file.

You cannot use this feature to restore multiple files. To search for and restore multiple files, please see the Advanced Filtering section below.

Restore a Microsoft SQL server

Overview: ZCB supports Simple Recovery Model, Full Recovery Model and Bulk Recovery Model for SQL server databases. You can restore to the original backed up system or a different system altogether.

Requirements for all database restores:

- Do not run backup and restore operations of a MS-SQL backup simultaneously.
- SQL 2005 restores of system databases, such as model, master, and msdb, will fail if other applications are actively connected to the MS-SQL server. Please disable any SQL query analyzers, the MS-SQL Management Studio, and other such programs before performing a restore of system databases.
- The SQL writer service must be running at the time of backup and recovery. Microsoft recommends that the SQL VSS Writer service be automatically started. MSDE writer is not sufficient for backup and recovery.
- The *amandabackup* user must be added as a SQL server user with sufficient privileges.
 - Click the "Allow Access" button on the Backup page of any Microsoft SQL backup set.
 - To add the user in SQL server Management Studio, click on Security > Logins > Add New Login. Add the *amandabackup* user account and give it privileges.
 - You can just add it to sysadmin server role.
- The log-on user for the SQL Server service must have full permissions to whatever folder is chosen for restore.



It is recommended that system databases, such as model, master, and msdb, be restored separately from user databases. System databases should be restored first.

Additional requirements for restore to another machine

Restore of SQL backups to an alternate server are supported as of ZCB 4.7. Backups from previous ZCB version 4.6 and earlier may also be restored to an alternate server that is running ZCB 4.7.

- The SQL Server instance name must be exactly the same on the new machine as it was on the original machine. The restore will fail if the instance names do not match.
- Restore of system databases such as master, model, and msdb require that the SQL Server version exactly match between the new machine and the original machine. The restore will fail if there is a version mismatch.
 - Example: The model database of a SQL Server 2005 database cannot be restored to anything other than a SQL 2005 instance.
- Restore of user databases require that the SQL Server version on the new machine be the same as or higher than the original machine.
 - Example: A user database from a SQL 2008 instance can be restored to another SQL 2008 instance or a SQL 2012 instance. It cannot be restored to a SQL 2005 instance.
- Restore of user databases require that the new machine be running the same or higher version of Windows operating system as the original.
 - Example: A SQL 2008 instance running on Windows Server 2003 can be restored to a SQL 2008 instance running on Windows Server 2003, 2008, or 2012.
 - Example: A SQL 2008 instance running on Windows Server 2008 cannot be restored to Windows Server 2003. It can be restored to Windows Server 2012.
- The **Restore a Copy of Database to Original or New Location** and **Restore to a New Location and Overwrite Original Database** options, discussed below, may both be used to restore to an alternate machine.

Special Options for database restores:

- **Point-in-time Restore:** Users can restore to any point in time if they take Incremental(log) backups. Select "Point-in-time" from the dropdown menu, then use the spinner to choose the specific time to which the restore should take place. This allows the database to be

restored to any time, even between backups.

- Use the spinner to select any time between the chosen Incremental(log) backup and the most recent Full backup.
- **Run DBCC CHECKDB After Restore:** This option checks the logical and physical integrity of all the objects in the specified database(s) after the restore completes.

Database Ownership After Restore

This section does not apply to restores to the Original Location.

The *amandabackup* user is used to initiate the restore operations for Microsoft SQL Server. It will thus become the new owner of the restored databases during restores to a different computer or different instance.

This is necessary for several reasons:

1. It cannot be assumed that the user who previously owned the database exists during the restore process.
2. The user performing the restore must have the necessary permissions to apply transaction log backups to the newly restored database.
3. Likewise, the user performing the restore must have full and total access to the database, including ownership changes.

Because we require that the *amandabackup* user be added as a Sysadmin, we know that the *amandabackup* user satisfies these requirements.

After restore, any system administrator can change the database ownership to any user. Please see this Microsoft Article for more information on how to change database ownership: <http://technet.microsoft.com/en-us/library/ms190909%28v=sql.105%29.aspx>

Restore locations

On the Restore page, you may choose where you wish to restore your database. Each option has special functionality designed to fill a specific purpose. Please review the options below.

Original Location

This will restore the selected databases to the location where it was originally located at the time of backup.



If the database to be restored is currently attached to the SQL instance, and the current location of the database files is *different* from the time of backup, then ZCB will treat the current database location as the "Original" location.

Restore a Copy of Database to Original or New Location

This method allows a user to restore the selected database with a new name to either its backup location or to a completely new location. This is similar to making a copy of the database with a new name to a new location.



SQL 2000 databases whose backups were taken with ZCB 4.6 or older cannot be restored with this method.

Information:

- SQL recovery is performed during the restore.
- The database file names (.ldf & .mdf) remain the same as before.

Requirements:

- System databases, such as master, model, and msdb, cannot be restored using this method.
- To restore the database to the Original location, the Path field must be blank.
- When restoring to the Original location using this method, the Original database must be deleted or detached from SQL before the restore begins.
 - If the Original database still exists, the restore will fail.
- Once a user makes a selection on the Restore page, he cannot make any changes to the selection list unless he toggles between Restore Methods.

Procedure to restore a copy of a database to its original location:

In the following example, we describe a database named 'Sales' that needs to be renamed as 'SalesTeam' and restored to its original location.

1. Go to the Restore page and select 'Sales' database in the File Path view.
 - a. It is not necessary to select the database in *all* of the full, differential, and/or incremental backup runs. If one selects the 'Sales' database in any one backup run, ZCB will automatically select 'Sales' database from all other backup runs that are required for restore.
2. From the 'Restore Method' drop down, select 'Restore a Copy of Database to Original or New Location' option.
3. The 'Edit Database Name & Restore Path' dialog box will appear.
 - a. Specify the new name 'SalesTeam' in 'New Name' field.
 - b. Keep the 'Path' field blank since we want to restore it to the same old location.
 - c. Save the changes.

4. (Optional) Select the 'Run DBCC CHECKDB' check box if you wish to verify the logical and physical integrity of all the objects in the specified database(s) after the restore completes.
5. Click on the Restore button.
6. A confirmation box will appear. Click OK to restore or Cancel to cancel.
7. After restore completes, the 'SalesTeam' database will appear in the SQL Management Studio

Procedure to restore a copy of a database to a new location:

In the following example, we describe how to make a copy of a database named 'Marketing' that originally exists at 'C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA' with a name 'MarketingTeam' that will be created at 'E:\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA'.

1. Go to the Restore page and select the 'Marketing' database in the File Path view.
 - a. It is not necessary to select the database in *all* of the full, differential, and/or incremental backup runs. If one selects the 'Marketing' database in any one backup run, ZCB will automatically select 'Marketing' database from all other backup runs that are required for restore.
2. From the 'Restore Method' drop down, select 'Restore a Copy of Database to Original or New Location' option.
3. The 'Edit Database Name & Restore Path' dialog box will appear.
 - a. Specify the new name 'MarketingTeam' in the 'New Name' field.
 - b. Click inside the 'Path' field and browse to the target folder
 - i. i.e. 'E:\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA'.
 - c. Save the changes.
4. (Optional) Select the 'Run DBCC CHECKDB' check box if you wish to verify the logical and physical integrity of all the objects in the specified database(s) after the restore completes.
5. Click on the Restore button.
6. A confirmation box will appear. Click OK to restore or Cancel to cancel.
7. After restore completes, both the 'Marketing' & 'MarketingTeam' databases will appear in the SQL Management Studio.

Restore to a New Location and Overwrite Original Database

This method allows a user to move the selected database to a completely new location.



This option may still be chosen if the original database is not present. The "Restore to a New Location and Overwrite Original Database" option will behave exactly like "Restore a Copy of Database to Original or New Location" in such a situation.



SQL 2000 databases whose backups were taken with ZCB 4.6 or older cannot be restored with this method.

Information:

- SQL recovery is performed during the restore.
- The database file names (.ldf & .mdf) remain the same as before.
- ZCB restores the database to the 'Path' specified by the user in the 'Edit Restore Path' dialog box.
- Details about the restore procedure are logged by the SQL Server in the Windows Event Viewer.

Requirements:

- System databases like master, model, and msdb cannot be restored using this method.
- If the selected database exists on the SQL server before the restore procedure, the database files from the original location will be deleted and restored to the new location.
- Once a user makes a selection on the Restore page, he cannot make any changes to the selection list unless he toggles between Restore Methods.

Procedure to Restore to a New Location and Overwrite Original Database:

In the following example, we describe a database 'Finance' that originally existed at 'C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA'.

This database needs to be moved to a new location at 'E:\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA'.

- Go to the Restore page and select the 'Finance' database in the File Path view.
 - It is not necessary to select the database in *all* of the full, differential, and/or incremental backup runs. If one selects the 'Finance' database in any one backup run, ZCB will automatically select 'Finance' database from all other backup runs that are required for the restore.
- From the 'Restore Method' drop down, select the 'Restore to a New Location and Overwrite Original Database' option.
- The 'Edit Restore Path' dialog box will appear.
 - Click inside the 'Path' field and browse to the target folder
 - i.e. 'E:\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA'.
 - Save the changes.
- (Optional) Select the 'Run DBCC CHECKDB' check box if you wish to verify the logical and physical integrity of all the objects in the specified database(s) after the restore completes.
- Click on the Restore button.

- A confirmation box will appear. Click OK to restore or Cancel to cancel.

Restore to an alternate location without Recovery (FULL Backups Only)

This method restores the SQL database files (.mdf & .ldf) to the specified location. It is available *only* for full backups taken with ZCB version 4.6 or earlier.

Information:

- No SQL recovery is performed during the restore.
- This is a simple file level restore.

Requirements:

- Only Full backups can be restored using this method. Differential and/or Incremental backups cannot be restored.
- Unlike the other SQL restore types above, you may use any machine name with any instance name.

Restore a Microsoft Exchange Server

Overview: In the event of a server loss, how you perform the recovery will depend on the server role and your disaster recovery plan. 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. Using ZCB, 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.

Functionality: Three types of recovery operations are allowed by Microsoft Exchange:

- Roll-forward
- Point in time
- Full restore

The state of the Microsoft 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.

All Exchange versions support restores to the Original location. In addition, you can restore Exchange 2007 backups to a Recovery Storage Group and Exchange 2010 or 2013 backups to a Recovery Database.

Requirements for all machines:

- 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, Exchange 2010).
 - For Exchange 2003 and 2007, *all* Mailbox Databases and Public Folder Databases within the target Storage Group must meet this requirement, even if a single database is being restored.
- The following prerequisites must be installed
 - .NET 4.0 or higher (Not required for Exchange 2003)
 - Powershell 2.0 or higher (Not required for Exchange 2003)

Additional Requirements (for restores to an alternate Exchange Server)

- Please complete the steps described in the [Restore to a different machine](#) section above.
- The target Exchange version and service packs must be the same 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.
- Because you are restoring to an alternate "recovery server" that has a different set of log files, 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.
- 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. Please refer to the [Requirements](#) section for how to do this.
- 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 **Microsoft Exchange Information Store Service**.
- In case of Windows 2003 Small Business Server edition, the Exchange Writer is disabled by default. Please follow the instructions this Microsoft knowledgebase article to enable the Exchange Writer: <http://support.microsoft.com/kb/838183>

Additional Requirements (for selective restores in Exchange 2003 and 2007)

It is possible to selectively restore individual Public Folder Databases and Mailbox Databases in Exchange 2003 and 2007.

- Public Folder Databases and Mailbox Databases can be restored to the Original location for both Exchange 2003 and 2007.
- Restore to a Recovery Storage Group is possible for Exchange 2007, but not for Exchange 2003.
- The Database Files *and* the associated Logs must be selected on the restore page.
- The **Delete existing transaction logs before running the restore** method (discussed below) is *not* allowed for selective restores to the original location in Exchange 2003 or 2007.
 - A **No Loss Restore - Do not delete existing transaction logs** restore will be performed for all selective restores, even if **Delete existing transaction logs** is selected.

Restoration to Original location: 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. Ensure that [all the requirements](#) are satisfied before starting the restore.

You will be presented with two options when you restore to the Original Location.

- **No Loss Restore - Do not delete existing transaction logs**
 - The existing transaction logs will not be deleted during the restore. Once the restore is complete, Exchange will perform a roll-forward recovery if all sequential transaction logs are found.
 - Because Public Folder Databases participate in replication by design, the **No Loss Restore - Do not delete existing transaction logs** method is not supported for any restores that include Public Folder Databases. The **Delete existing transaction logs before running the restore** method must be chosen.
- **Delete existing transaction logs before running the restore**
 - This is a "Point in time" recovery method.
 - All transaction logs that are currently present in the **Log directory** of the Storage Group(s), to which restored Mailbox Database(s), Public Folder Database(s), and/or Storage Group(s) belong, will be deleted at the beginning of the restore process.

Next, perform these steps to restore an Exchange server data to original location.

- Navigate to the Restore page in the ZCB user interface. Select the backup and point in time that you want to restore.
- Select the Mailbox Store Database or Public Folder Database & its associated Logs from the File List view.
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made.
- From the drop down select - "Restore Policy: Overwrite Original". Once confirmed, click Restore to start the restore process.

Restoration to Alternate Exchange 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).

The steps to restore an Exchange server data to an alternate Exchange server are:

- Navigate to the Restore page on ZCB user interface. Select the backup and point in time that you want to restore.
- Select the Mailbox Store Database or Public Folder Database & its associated Logs from the File List view.
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made. In case of a Recovery Exchange server, the data will be restored to the newly created Mailbox/Public Folder store.
- From the drop down select – "Restore Policy: Overwrite Original". Once confirmed, click Restore to start the restore process.

Restoration to Recovery Storage Group/Database: Microsoft Exchange Server allows recovery to a Recovery Storage Group in Exchange 2007 and to a Recovery Database in Exchange 2010 & 2013.

With Recovery Storage Groups and Recovery Databases, users can restore the Mailbox Store to a production Exchange Server without dismounting the Mailbox stores.

Restoring to a Recovery Storage Group/Database is not supported for Exchange 2003.



Restoration of a Public Folder Database to a Recovery Storage Group or Recovery Database is not supported by Exchange. Any attempt to do so will result in a failed restore with the error "Restore could not proceed as VSS initialization failed."

Further details about the failure can be found in the Windows Application Event Logs.

To restore to a Recovery Storage Group or Database, ensure that the following requirements are met by the Exchange server:

- The Recovery Storage Group or Recovery Database must be created *before* restore using the Exchange Management Tool or the Exchange Management Shell.
- All of the recovery databases in the Recovery Storage Group must be dismounted.
- All of the recovery databases must have the "This database can be overwritten by restore" option enabled.
- The Recovery Storage Group or Recovery Database folder must be empty.

In ZCB, perform these steps:

- Navigate to the Restore page on ZCB user interface. Select the backup and point in time that you want to restore.
- Select the Storage Group or the Mailbox Store Database and its associated logs from the File List View.
- Select the radio button - "Restore to Recovery Database".
 - For Exchange 2007, enter the name of the Recovery Storage Group
 - For Exchange 2010 & 2013, enter the name of the Recovery Database
- Click Restore to start the restore process.
- After you confirm your choices, ZCB will restore the data to folder in which the Recovery Storage Group or Recovery Database resides.



If you are restoring to a different machine:

- The name of the new machine must exactly match the name of the old machine.
- The recovery server must have the same Organization name, same Storage Group name, and same Mailbox or Public Folder

database name as the original server.

How to recover a deleted mailbox or a mailbox item: It often happens that a mailbox or mailbox items like emails/folders get accidentally deleted. Microsoft Outlook provides users a way of recovering the deleted folder items by using the [Recover Deleted Items](#) option. To recover a deleted Mailbox within the mailbox retention period, one can reconnect the user account to the deleted mailbox using the [Exchange Tasks](#).

In case none of the above recovery options work i.e. when the deleted mailbox has an expired mailbox retention period, one is left with no other choice but to restore the Exchange server Mailbox store to a recovery server or to a recovery database. Follow the steps mentioned in the **Restoration to Alternate Exchange Server** or **Restoration to Recovery Storage Group/Database** to restore the Mailbox store database which has the deleted mailbox. Additionally use the [Exmerge.exe](#) to extract the data from the restored Mailbox store to a .PST file as follows:

- Using the Exchange System Manager or Exchange Management Console, 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. Launch the Exmerge.exe. Select the **Extract or Import (Two step procedure)**.
- On the next screen, select **Step 1: Extract data from an Exchange Server Mailbox**. This will step extract the data from the desired mailbox into a .PST file.
- Copy the .PST file to the production Exchange server where the deleted mailbox originally existed.
- 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: Import data into an Exchange Server Mailbox** to import the data from the .PST file into the desired mailbox. All the deleted items should be now recovered.

Restore Microsoft SharePoint

Overview: ZCB supports Content Recovery, Web Application Recovery and Disaster Recovery for Microsoft SharePoint. You can restore to the original backed up system or a different system altogether.

Functionality:

- **Content Recovery**

Content recovery applies to being prepared for accidental updates or deletions of data, usually by end users such as deleting documents, tasks, calendar 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.

- **Restoration to Original location:** ZCB performs the restore to original location in following steps:
 - 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
 - The selected SharePoint database/s and log file/s are restored to their original location. If all the data is selected from the Restore page, all the databases and Index search files are restored. You can also select individual content databases to restore.
 - 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.
 - The services which were stopped before the restore operation are restarted.
- **Restoration to Alternate location:** 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.



If you are restoring to a different machine:

- The name of the new machine must exactly match the name of the old machine.
- The instance name must match the name from the original server.

Requirements:

- If you are attempting to restore data to a different machine than the one which was backed up, please complete the steps described in the [Restore to a different machine](#) section above.
- The target server must have the same SharePoint server (WSS 3.0 or MOSS 2007 or Share Point 2010) with same Service Packs and SQL server (embedded SQL server or SQL server 2008 or SQL server 2005 or SQL server 2000).
- Make sure that Microsoft 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.
- The Share Point Databases must be in stable state. To check the state of the SQL server, Connect to the SQL server using MS SQL Management Studio. The **Properties** from right click menu for each database will display the state. The state of the database must be **Normal**.
- Please make sure that the following services are in the **Started** state- Windows SharePoint Services VSS Writer- Volume Shadow Copy-

Restore Windows System State

Overview: ZCB offers recovery of Windows System State on all the supported Windows platforms.

Functionality: ZCB supports backup of Windows System State and performs VSS based backup of Boot files, System files, IIS, COM+ database, Registry, Active Directory and Certificate Server. Windows System State is always a full backup.

Please note that for system state restores, ZCB will set default values which are different from those of other applications. It will set the **Restore to** option to **Original Location** and the **Restore Policy** option to **Overwrite Original**.



the more dissimilar the hardware from the original, the less likely the system state restore will be successful.

Requirements:

- You must install the same Windows Operating System (with the same service packs) on the restore machine as was installed on the original machine.
- If you are attempting to restore data to a different machine than the one which was backed up, please complete the steps described in the [Restore to a different machine](#) section above.
- The Volume Shadow Copy Service must be enabled. Please refer to the [Requirements](#) section.
- For restore of a Windows server running Active Directory, please refer to [Performing System State restores on Windows SBS 2011](#).

Restore a MySQL Server

Overview: The Restore page for a MySQL backup set presents users with 2 views namely **Databases** and **SQL Files**. To select databases, use the **Databases** view. ZCB allows selecting individual databases but does not support selecting individual tables for restore. The **SQL Files** filter shows the *backup.sql* containing SQL commands.

Functionality: The same MySQL server information and MySQL user credentials for the backup set (as configured in the **Backup What** page) is used for restoration.

The steps to restore MySQL database or tables to the Original server are:

- Navigate to the Restore page on ZCB user interface. Select the backup run you want to restore from.
- Use the **Databases** view and select the databases to be restored.
- Click on **Restore**.
- The backup image containing SQL commands is restored to the **Restore Location** specified in Restore page.
- The **Policy** in the Restore page is applied to the files in this location (not MySQL databases/tables).
- The *mysql* client command is then used to execute the SQL commands that are in the backup image. ZCB will restore the selected databases or tables to the MySQL server from where the backup was taken from.

The steps to restore the MySQL backup file are:

- Navigate to the Restore page on ZCB user interface. Select the backup and point in time that you want to restore.
- Use the **SQL Files** view and select the backup.sql file and its folder.
- Click on **Restore**.
- When MySQL file is restored using this procedure, no MySQL recovery is performed.
- The MySQL backup image contains sequence of MySQL commands that can bring the database back to original state. Restoration of the backup.sql file allows users to edit the SQL commands and run a manual recovery as needed.

Requirements:

- 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.

Restore an Oracle Server

Overview: In the event of a server loss, how you perform the recovery will depend on the server role and your disaster recovery plan. One would also need to recover Oracle databases in case of issues such as database deletion/corruption, loss of control files, etc. Using ZCB, Oracle database can be restored to the same server or to an alternate server depending on the Disaster Recovery plan.

Functionality: There could be various scenarios when Oracle data would need to be restored. Once ZCB copies the data to the desired location, user needs to run recovery commands using **sqlplus** to get the database in consistent state. Below are some recovery scenarios where database files, control files, etc have been accidentally deleted/corrupted.

The steps to restore all Oracle datafiles (Disaster Recovery) in **Archivelog** to the Original location are:

- Ensure that the instance is not started.
- Navigate to the Restore page in the ZCB user interface. Select the backup run you want to restore from.
- Select the database files to be restored i.e. the datafiles, server parameter file, etc. In case the redo logs are missing, select the appropriate archived redo log files as well.
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made.
- From the drop down select – "Restore Policy: Overwrite Original". Once confirmed, click Restore to start the restore process.
- Click on **Restore**.
- Once the database is successfully restored, open the **sqlplus** and run the below commands.

```
cmd> sqlplus /nolog
sql> connect sys as sysdba
sql> shutdown immediate
sql> startup mount
sql> recover database using backup controlfile until cancel;
```

Note: In cancel-based recovery, recovery proceeds by prompting you with the suggested filenames of archived redo log files. Recovery stops when you specify CANCEL instead of a filename or when all redo has been applied to the datafiles.databases/tables).

- Continue applying redo log files until the last log has been applied to the restored datafiles, then cancel recovery by executing the following command:

```
sql> CANCEL;
```

- To finish, enter the following SQL command string

```
sql> alter database open resetlogs;
```

- 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;
```

The steps to restore a single Oracle datafile in **Archivelog** to the Original location are:

- Ensure that the database is either mounted or open. If the database is open, run sqlplus on Command Prompt and connect to the database.

```
cmd> sqlplus sys as sysdba
```

- To recover the datafile, the tablespace needs to be taken offline. Lets consider an example where the tablespace ZTEST01 needs to be restored.

```
sql> ALTER TABLESPACE ZTEST01 OFFLINE IMMEDIATE;
```

- Navigate to the Restore page on ZCB user interface. Select the backup run you want to restore from.
- Select the datafile to be restored i.e. ZTEST01.dbf in our example. In case the redo logs are missing, select the appropriate archived redo log files as well.
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made.
- From the drop down select – "Restore Policy: Overwrite Original". Once confirmed, click Restore to start the restore process.
- Click on **Restore**.
- Once the database is successfully restored, open the **sqlplus** again and run the below commands.

```
cmd> sqlplus /nolog
sql> connect sys as sysdba
```

- If the restored data file is older than the redo log files, then a media recovery needs to be initiated using the below command:

```
sql> RECOVER TABLESPACE ZTEST01;
You will see the below message
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
```

- Input the appropriate log file location. Type 'AUTO' if you want Oracle to automatically find the appropriate logs and apply it.

```
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
AUTO
Log applied.
Media recovery complete.
```

- Once you have recovered all the tablespaces that you have lost, bring the offline datafile or tablespace back online using command:

```
sql> ALTER TABLESPACE ZTEST01 ONLINE;
```

The steps to restore the server parameter file are:

- Navigate to the Restore page in the ZCB user interface. Select the backup run you want to restore from.
- Select the Server parameter file (spfile) to be restored. Usually, it is named as **SPFILE"ORACLE_SID".ORA** . For example, if the SID of the database is "ORCL", then the name of spfile will be "SPFILEORCL.ORA".
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made.

- From the drop down select – "Restore Policy: Overwrite Original". Once confirmed, click Restore to start the restore process.
- Click on **Restore**.
- Once the restore operation is done, run sqlplus on Command Prompt

cmd> sqlplus sys as sysdba

- Shutdown the database and startup again.

sql> SHUTDOWN immediate

sql> STARTUP

- Check the database whether it's up and running

sql> SELECT name, open_mode from v\$database;

The steps to restore all datafiles in **NoArchivelog** are:

- Navigate to the Restore page in the ZCB user interface. Select the backup run you want to restore from.
- Select all the datafiles & control files. ZCB backs up one of the 3 control files i.e. **CONTROL01.CTL**.
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made.
- From the drop down select – "Restore Policy: Overwrite Original". Once confirmed, click Restore to start the restore process.
- Click on **Restore**.
- Make two extra copies of the **CONTROL01.CTL** file called **CONTROL02.CTL** and **CONTROL03.CTL**. For your information, **CONTROL01.CTL** file is located in the **ORAHOME\ORADATA\DATABASE_SID** directory.
- To run the recovery, run sqlplus on command prompt:

cmd> sqlplus /nolog

sql> connect sys as sysdba

sql> shutdown immediate

sql> startup nomount

sql> ALTER DATABASE mount;

sql> RECOVER DATABASE;

sql> ALTER DATABASE open;

The steps to restore all Control files in Archivelog are:

Note: When Oracle database control files are backed up by Volume Shadow Copy Service, the backed-up files are referred to as Snapshot Control files. For example, a control file by the name of 'CONTROL01.CTL' is backed up under the name SNCFDATABASE_SID.ORA. Let's consider an example where the database SID is ORCL. In this case the snapshot control file will have the name SNCFORCL.ORA.

- Ensure that the database is in NOMOUNT state or can be started in NOMOUNT state by the Oracle VSS writer. You don't have to shut down the database manually.
- Navigate to the Restore page on ZCB user interface. Select the backup run you want to restore from.
- Select the snapshot Control File. In the above case, select 'SNCFORCL.ORA' since the SID of the database is ORCL.
- Select the radio button - "Restore to Original Location." ZCB will restore the data to the same location from where the backup was made.
- From the drop down select – "Restore Policy: Overwrite Original".

Once confirmed, start the restore process.

- Click on Restore.
- SNCFDATABASE_SID.ORA file is located in the 'ORAHOME\product\db\database\'

directory. Example, it would be located in the 'C:\app\Administrator\product\11.1.0\db_1\database\' directory.

Note: ZCB automatically stops the Oracle instance while restoring and then starts it again when the restore operation is finished.

- Make three copies of the SNCFDATABASE_SID.ORA called CONTROL01.CTL,

CONTROL02.CTL, and CONTROL03.CTL.

- Copy these three files to the control files install location. The default location is 'ORAHOME\oradata(DATABASE_SID)\'. For the above example, copy the files to the 'C:\app\Administrator\oradata\ORCL\' directory.
- Run sqlplus on Command Prompt Window

cmd> sqlplus sys as sysdba

- Shut down the database and startup

sql> SHUTDOWN IMMEDIATE

sql> STARTUP MOUNT

- Run the below command to get the database in consistent state.

sql> RECOVER database using backup controlfile until cancel;

- Continue applying redo log files until the last log has been applied to the restored datafiles, then cancel recovery by executing the following command:

sql> CANCEL;

- Open the database with the RESETLOGS option.

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;

Requirements:

- If you are attempting to restore data to a different machine than the one which was backed up, please complete the steps described in the [Restore to a different machine](#) section above.
- Please make sure that the following services are in the Started state- Oracle VSS Writer- Volume Shadow Copy

Restore Hyper-V

Overview: ZCB supports backup and restore of Hyper-V hosts and hosted virtual machines on Windows 2008, 2012, and 8.

Functionality:

- Users may select individual virtual machines for restore.
- Restore may be done to the original location or an alternate location.
- Restore to the original location cannot overwrite an active, running VM. If such a restore is attempted, it will be interrupted with this warning:

```
The guest VM that you are trying to restore to appears to be in running state. It will be turned off during the restore.
```

```
Are you sure you want to continue?
```

```
OK  Cancel
```

Select "OK" to turn off the running VM and continue the restore. Select "Cancel" to abort the restore process.



The above warning will **not** be issued if the Virtual Machine's name has changed since the backup was taken, even if the VM is running. ZCB will proceed directly with the restore.

This will remove the existing VM and replace it with the backup VM.

Requirements:

- You **must** install the same Windows Operating System (with the same service packs) on the restore machine as was installed on the original machine.
- If you are attempting to restore data to a different machine than the one which was backed up, please complete the steps described in the [Restore to a different machine](#) section above.
- The Volume Shadow Copy Service must be enabled. Please refer to the [Requirements](#) section.

Locate A Backed Up File

This option allows you to search for a file **across all backup runs** for a backup set and restore its latest version quickly. This can be useful when you have a lot of backup runs and don't remember which backup run contains the file you need.

After clicking the **Locate A Backed Up File** button, simply enter as much of the file name or the file path as you remember. ZCB will search for this in all the backup runs and return a list of all files and directories that contain the name you entered and the most recent time they were backed up.

You can select the file from this result window and click on the "Select this file for Restore" button. Then provide your restore preferences in the main Restore page, and hit Restore button to restore the latest version of this file.

You cannot use this feature to restore multiple files. To search for and restore multiple files, please see the Advanced Filtering section below.

Advanced Filtering

To filter items, users may specify patterns that include wildcards, combine them with 'and' or 'or', as well as apply negation to the whole pattern. The syntax for the pattern expressions is as follows:

- "Or" filtering = pattern||pattern
- "And" filtering = pattern&&pattern
- "Not" filtering = !pattern
- "Exact" filtering = "pattern"
- The pattern may contain any **alphanumeric characters, path separators** (only backward slashes), or **any characters that are valid in**

a file path name

- ZCB automatically searches for any result that includes the submitted string.
 - For example, if the word **test** is submitted, all files and directories that contain **test** will be returned.
 - If the submitted string contains an asterisk *, the asterisk will be used as a wildcard.
 - If no wildcards are used, any result that matches the string will be returned.
- Absolute paths can be specified as follows: **C:\Users\FileServer*.txt** or **C:\Users\FileServer**.

Examples of OR:

- **jpg|txt|docx** to show either jpg, txt, or docx files.
- **C:\Users\FileServer*.txt|.docx** to show any .txt files in C:\Users\FileServer **or** any .docx files in any directory.

Examples of AND:

- **C:\Users&&jpg** to show all jpg files in the C:\Users directory.
- **Products&&TestData** to show all files that are both in the Products directory and the TestData directory.

Examples of NOT:

- **!pdf** to show all files that are not pdf.
- **!Users** to show all files that are not in the Users directory.

Examples of EXACT:

- **"C:\Users\"** to show the C:\Users\ directory.
- **"MSSQL-2005:\WINDEV-REPLACE\MSSQLSERVER\A1"** to show the MSSQL-2005:\WINDEV-REPLACE\MSSQLSERVER\A1 database.

Disaster Recovery

Disaster recovery refers to restoring the system and data in the event of partial or complete failure of a computer because of natural or technical causes. The following sections explain how to prepare for Disaster Recovery of any application server running Microsoft SQL server, Microsoft Exchange server, Microsoft SharePoint server or any File server and then how to recover the system in case of a disaster.

Preparing for Disaster Recovery

To protect an application Server from a disaster, one should perform backups of its critical components like System State, application data like databases, application installation directories, etc. We recommend users to create backup sets for such critical components like:

- **System Drive (default: C:)** - Exclude all system and temporary files. This is the drive where the Windows operating system and all applications are installed.
- **System State** - Backup of the server's registry, boot files, COM+ database, Active Directory, etc.
- **Application data** – Application data backup like Microsoft SQL server, Microsoft Exchange server, Microsoft Sharepoint server.
- **Application installation directory** - if the application is installed on a drive other than the System drive, include the installation directory. You can exclude the Database directory since it will be backed up as a part of SQL server database backup.
- **User Data** - Backup of File server data on partitions other than the System drive.

Performing Disaster Recovery

- Install the same version of Windows server and Service Packs as the original server. Make sure that the new server has exact same drive partitions, Windows installation directory and Computer Name as the original server. Do not put the machine in any domain or Workgroup.
- Log in to the machine as an Administrator.
- Install ZCB in the same directory location as the original server.
- Since you are attempting to restore data to a different machine than the one which was backed up, please complete the steps described in the [Restoring the Backup Catalog](#) section to download the catalog of backup sets uploaded from the original server.
- Restart the ZCB UI upon a successful completion of Restore Catalog procedure.
- Activate the backup sets using **File Menu > Activate Backup Set**.
- Click on the System drive backup set. Navigate to the **Restore** page on ZCB user interface. Select the backup and point in time that you want to restore.
- Select the radio button - "**Restore to Original Location**" ZCB will restore the data to the same location from where the backup was made.
- In the drop down menu select "**Restore Policy: Overwrite Original**". Once confirmed, click **Restore** to start the restore process.
- The restore of the System drive may report errors, since it will be unable to restore the Windows system files. You can safely ignore failure for these system & open files.
- After the System drive data has been successfully restored, restore the data for **System State** backup set with similar restore settings as above.
- The next data to be restored is for the **Application installation directory & User Data** backup sets with similar restore settings as above.
- Now reboot the server.

- After the server is rebooted, go to the Windows Services and check if the application services are installed and in a running state.
- Once the application services are confirmed as running, restore the **Application data** backup set.

Administration

Advanced Options

The Advanced Options menu can be found under **Preferences > Advanced**.

Data Transfer and Networking

A proxy server for data transfer to and from the cloud if IT policies require it. Please see [How to configure ZCB to work with authenticated proxy servers](#) if your proxy server requires authentication.

- **Proxy Host:** Enter the proxy server's host address.
- **Proxy Port:** Enter the port used for access to the proxy server.

ZCB listens on ports 10080 and 10081 and requires these ports. If you want to change the ports, specify them here.

- **Backup Port:** Enter the port used to upload data to the cloud during a backup.
- **Restore Port:** Enter the port used to download data from the cloud during a restore.

 The above ports have nothing to do with your firewall configuration. You do not need to open these ports for inbound connections.

On a related note, ZCB connects to port 443 and 80 of the cloud storage service. These ports must be opened for outbound connections in the firewall.

If you change the ports, you must restart ZCB background services. Click **Tools > Restart Background Services...**

When ZCB transfers data to and from the cloud, it opens multiple connections to the cloud server. Each connection is known as a "thread". Depending on your system resources and available upload bandwidth, you may be able to improve data transfer speeds by increasing the thread count. However, using more threads than necessary may cause slower transfers or other undesirable effects. The default number of threads is **3** and can not be higher than **10**.

- **Max. Download Threads:** Use this setting to change the number of threads used by ZCB when downloading data from the cloud.
- **Max. Upload Threads:** Use this setting to change the number of threads used by ZCB when uploading data to the cloud.

 Changes made to the number of transfer threads will only apply to future transfers. They will not affect current transfers.

Retention Policy Enforcement

Every day, ZCB will check for backups that have met their retention policy and purge them.

- **Purge old backup data every day at:** Choose the time at which ZCB will purge old backups.
 - Please see [Retention Policies](#) for more information on retention and purging.

The Report page shows old backups, even those that have been purged.

- **Keep expired backup run reports for:** Set the length of time ZCB will display reports of old backup runs.

General

ZCB uses the following folders for different purposes. You can change these folder locations to suit your needs.

- **Temporary Directory:** ZCB saves temporary files created during backups to this directory.
- **Backup Directory:** Backups are saved to this directory in a folder with the name of the backup set.
- **Download Directory:** During a restore, backup archives are saved to this directory.
- **Restore Directory:** When restoring to an alternate location, files are saved to this directory.

 Changes made to the **Temporary Directory** setting will not take effect until ZCB services are restarted. Please click on **Tools > Restart Background Service** from the top menu bar.

 Changes made to the Backup Directory setting will only apply to **new** backup sets. Existing backup sets will use the previous Backup Directory.

To change the Backup Directory for existing backup sets, please use the `movebackup` command.

A special Windows user named *amandabackup* is created when ZCB is installed.

- **amandabackup user:** Click the button to [update the amandabackup user password](#).

Localization

ZCB is available in 6 languages – English, German, Japanese, Simplified-Chinese, Traditional-Chinese and Korean. However to use file/folder name containing non English characters, you need to have the Windows edition for that language. For example, if there are Japanese characters in file names to be backed up, you need to be running a Japanese edition of Windows operating system.

Email Notification

ZCB allows users to receive notifications when particular operations get completed. This control is offered both at the global level (for all backup sets) or at a backup set level.

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, such as the success or failure of a backup, upload, download, or restore operation.

To enable email notifications, you need to configure the mail server first. To do this, please click on **Preferences > Email...** and provide information for these fields:

- **From:** Please specify what mail id you would like ZCB to put in the **From** field of the emails. By default, this is ZCB-noreply@zmanda.com
- **To:** Input the email addresses to which you would like notifications to be sent. Separate multiple email addresses with a ";" (semi colon) character.
- **Outgoing SMTP Server:** This is the IP address or hostname of your outgoing SMTP server.
- **Port:** This is the SMTP server port which ZCB should connect to for sending emails.
- **Username:** This is the email address/username which is to be used for authentication with the mail server.
- **Password:** This is the password for the above email account.
- **Authenticate:** This check box is to be disabled if your SMTP server doesn't need authentication. Otherwise, please keep it enabled.
- **Secure:** If you want the communication between ZCB and SMTP server to be secured rather than clear text, select the appropriate option from the drop-down box. 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>

After entering correct values for above, you can test if ZCB can connect to the SMTP server by clicking on the **Send Test Mail** button.

Once you complete the above steps, you have successfully configured mail server. Now, you need to define email recipients list and what events you wish to be notified about. You can do this at both global and backup set levels.

Global Email Notifications

To add a global email list which can be used across all backup sets, please click on **Preferences > Email...** and provide a list of email ids. Multiple email addresses can be used if separated by a ";" (semi colon) character. If you don't want to define this global email list, you can skip this setting.

Once you add this list and have a working mail server configuration, by default ZCB starts sending notification of all success/failure events to this global email list. If you wish to modify this behavior at the backup set level, please refer to the Backup-set Specific Email Notifications section below.

Backup-set Specific Email Notifications

You can also control the email notification behavior at the backup set level and define what events and email-ids are used for notification by ZCB.

To do this, select the backup set from the left hand pane and go to **Backup** page. In the **Backup When** section, under the **Backup Set Preferences** tab, you can provide the value of the following fields:

Email Addresses: In this option field, you can specify email addresses which are specific to this backup set. Like before, multiple email addresses must be separated by a ";" (semi colon) character.

Also notify recipients specified in email preferences: By default, this check box is enabled which means that ZCB includes the global email list (as defined in the [Global Email Notifications](#) section above) in the notification emails generated by it. You can disable this checkbox, which will make ZCB send emails to only the email addresses defined in the **Notify** field above.

Event types: You can enable or disable checkboxes defining each event type for which you want to generate email notifications.

An example email reporting Upload success for backup set **BackupSetSystemState**.

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

Purge All Backup Runs Before...

ZCB also provides a method to remove all backup data before a specific date. This method is most useful when you wish to delete a large number of backup runs based on age, or if data is present on the cloud but not within ZCB.

1. Click on File -> **Purge All Backup Runs Before...**
2. A dialogue box will appear with several options.
 - a. Choose a date. All data prior to that date will be deleted.
 - b. Choose if you wish for data to be deleted from the cloud, from local disk, or from both.
 - c. Choose if you want to delete data from the currently-selected backup set only or from all backup sets.
3. A pop-up appears to confirm your decision.
4. ZCB will begin deleting your data.
 - a. All data older than the specified date will be deleted for the specified backup set.
 - i. If "all backup sets" was chosen, any data from the current machine that is older than the specified date will be deleted.
 - b. This operation requires communication with our cloud storage partners and can take a very long time, depending on the amount of data being removed. Please be patient.
5. A message will pop up once the operation is complete.

Upgrading ZCB

To check if there is a new ZCB version available, please go to **Help > Check for Updates**. You will be taken to the ZCB release page on Zmanda Network. From there, you will be able to download the new version, if available.

Reinstalling ZCB

If for some reason, you wish to reinstall ZCB on the same machine, you can do so by following these steps:

1. Click on **Windows Start > All Programs > Zmanda > Zmanda Cloud Backup > Uninstall** on the ZCB machine to launch the uninstaller.
2. If you wish to retain ZCB configuration and backup data on your machine, choose **Yes** when the uninstaller asks you this question.
3. In case you encounter uninstallation issues and wish to clean the ZCB state completely, follow the steps mentioned in the section below. Run the ZCB installer again and complete the installation

Cleaning up ZCB installation

If you are trying to uninstall ZCB and facing trouble, then please follow the following steps to clean up:

1. Locate the ZCB installer (.exe) which you downloaded from Zmanda Network.
2. Please right click on the installer and extract it as a zip archive using an archiving tool such as 7zip.
3. After extracting, open Windows command prompt and change to the extracted directory. Now, run one of these commands (require "Administrator" privileges)

ZCBInstallCleanUp.exe (If you wish to preserve ZCB data)

ZCBInstallCleanUp.exe -D (If you wish to force delete the full ZCB installation)

Cloud Storage

Checking the Cloud Connection and Subscription

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

Managing Amazon S3 Storage

This heading applies to ZCB with Amazon S3 Storage *only*.

Choose **Cloud > Purchase Cloud Subscription** or **Cloud > Manage Cloud Subscription** to open a browser window that connects you to Zmanda Network and the Amazon S3 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.

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

Managing Google Cloud Storage

This heading applies to ZCB with Google Cloud Storage *only*.

Each ZCB with Google Cloud Storage account has a limit, chosen at purchase, on the amount of data that can be stored in the cloud.

View an account's current usage by clicking **Cloud > Check Usage**.

Purchase more storage by clicking **Cloud > Buy More Storage**.

Import Cloud Certificate

After purchasing a subscription, the ZCB certificate will be available in your Zmanda Network account. Download the certificate from Zmanda Network to the ZCB machine. The ZCB certificate should be named *cloud.zmanda* and must be imported into the ZCB User interface using the **Cloud > Import Cloud Certificate** menu option.

There can be only one Cloud certificate installed for a ZCB installation.

Restore Catalogs

Found in the **Tools** menu, this option allows you to "import" backup sets from another ZCB installation.

When ZCB backs up data, it stores some key meta-information in a special file called the backup catalog. This catalog is used by ZCB at restoration time to let the user select the desired specific data for restoration and to restore the backup data correctly. This catalog is created for every successful backup.

Restoration of data to a machine other than the one that performed the backup (such as in a "bare metal" disaster recovery) requires that the Backup Catalog be restored first. After you have restored the backup catalog, you may browse backup sets, backup reports and perform data recovery.



You **must** close Zmanda Cloud Backup and restart it after the Restore Catalog process completes.

How to restore the backup catalog

1. Install ZCB to the new machine and import the ZCB certificate as mentioned in the [Importing the cloud certificate](#) section above.
2. Click **Tools > Restore Catalog**. Choose if you wish to restore the catalog from the cloud or from a local disk backup. See below for details.
3. Enter information about the backups you wish to recover and press "OK".
4. Your backups will be imported into ZCB. Imported backup sets will appear on the left side of the screen.
5. Select a backup report. You can now manipulate the backup set as you would any other. All functions, including reports and data restores are available.

Restore Catalog from Cloud

When restoring the catalog from the cloud, ZCB must search your cloud backups and download them. The more backups you have, the longer this process will take.

Therefore, ZCB will ask for information about the backup set(s) you wish to restore. The more information you enter, the faster ZCB will be able to restore the backup catalog.

- **Cloud Location:** ZCB can back up your data to data centers across the globe. The default selection is "All Cloud Locations."
- **Host Name:** This refers to the host name of the original machine, without the domain name (if any).
 - For instance, if your original machine's host name was *myexchangeserver.xyz.com*, please provide the host name as "*myexchangeserver*".
 - If you don't remember the original machine host name, then you can put the wild card * in this field. This will download catalog for all of the machines which were backed up using ZCB.
 - If you leave this field blank, ZCB will use the hostname of the machine on which it is installed.
- **Backup Set Name:** This refers to the name of the backup set on the original machine when the backup was taken.
 - If you wish to restore catalog for all backup sets, you may leave this field blank.
 - You can also use the wild card * to select matching backup set names.

- For example, entering **exchange*** will import all backup set names that begin with **exchange**, such as exchangebackup, exchangeone, etc.
- The backup set name field is case sensitive.
- **Restore Location:** If you wish, you can provide a temporary location on the local machine where the restored catalog will be stored by ZCB.

Restore Catalog from Local Directory

You can restore the backup catalog from backups kept on a local disk. If you have many backups on the local disk, filter using the **Host Name** and **Backup Set Name** fields.

- **Host Name:** This refers to the host name of the original machine, without the domain name (if any).
 - For instance, if your original machine's host name was *myexchangeserver.xyz.com*, please provide the host name as "*myexchangeserver*".
 - If you don't remember the original machine host name, then you can put the wild card * in this field. This will download catalog for all of the machines which were backed up using ZCB.
 - If you leave this field blank, ZCB will use the hostname of the machine on which it is installed.
- **Backup Set Name:** This refers to the name of the backup set on the original machine when the backup was taken.
 - If you wish to restore catalog for all backup sets, you may leave this field blank.
 - You can also use the wild card * to select matching backup set names.
 - For example, entering **exchange*** will import all backup set names that begin with **exchange**, such as exchangebackup, exchangeone, etc.
 - The backup set name field is case sensitive.
- **Backup Data Location:** The directory in which the local backups are stored.

Moving local backup data to a different location on the same machine

If you have been using ZCB to keep backup data on your local disk and now wish to move this old data to a new location on your machine (a different drive for instance), you can do so. For this, you will have to use the **movebackup** option of **zwcontroller.exe** program which ships with ZCB.

The syntax for this command is:

```
<Installation Folder>\bin>zwcontroller.exe movebackup <BackupSet> <BackupFolder>
```

Here,

- **Installation Folder** refers to the location where ZCB has been installed. By default, this location is **C:\Program Files\Zmanda\Zmanda Cloud Backup**.
- **BackupSet** refers to the string – "ComputerName+BackupSetName". So for instance if the backup set is MyDocuments and the computer name where ZCB is installed is zmandazcb.xyz.com, then the BackupSet string will be "zmandazcb+MyDocuments".
- **BackupFolder** refers to the complete path of the destination folder where the backup files are desired to be moved.

For example, let's assume that you have installed ZCB at the default location on a machine named "zmandazcb". To move backup data belonging to backup set "MyDocuments" to a new location "D:\ZCB-Backups", the command would be:

```
C:\Program Files\Zmanda\Zmanda Cloud Backup\bin>ZWController.exe movebackup "zmandazcb+MyDocuments" "D:\ZCB-Backups"
```

Please note the following for this operation:

- If there is any ongoing backup or upload operation for the backup set, the command will fail.
- You might also want ZCB to write new backup data to the new disk location. To do this, please change the **Location** field accordingly under the **Local Storage** heading in the **Backup Where** section.

Changing Log Level

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 the 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\<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. You can customize the amount of log messages ZCB generates. Generally, you would like to increase log level when you want to troubleshoot an issue or just before opening a support case.

To change the log level, please go to **Help > Change Log Level** and choose one of **Error, Warning and Debug**. The value **Debug** makes the logging most verbose and value **Error** makes it the least verbose.

Collect Logs

If you run into a problem that requires assistance, navigate to **Help > Collect Logs** before contacting the Zmanda Support Team. This makes ZCB collect all the relevant files into an archive, displaying its name and location. Please be patient as collecting the logs can take a few minutes and attach the log file to your support request. Please note that:

- Collect Logs has to be run as a user with Administrator privileges. If ZCB UI is being run as a user who is not an Administrator on Vista, Windows 7 or Windows 2008 server, a 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 a 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.

Original Location

Rename Database and Restore to Original or New Location

Restore Database to a New Location