

***Auto*VAULT®**

Installation and Users Guide

Version 3

Revised: October 2009

© Copyright Code Relief LLC 1999-2010. All rights reserved.

Code Relief, LLC

301 Rivervale Road

Reading, PA 19605 USA

Phone: 1-610-926-2556

Fax: 1-610-926-7178

email sales: [sales@coderelief.com](mailto:sales@coderelief.com)

email technical support: [tech@coderelief.com](mailto:tech@coderelief.com)

<http://www.coderelief.com>

## Trademarks

AutoVAULT is a registered trademark of Code Relief LLC in the United States and/or other countries.

AIX and IBM are trademarks of International Business Machines Corporation in the United States and/or other countries.

Tivoli and Tivoli Storage Manager are trademarks of Tivoli Systems Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, Windows 2000, Windows XP, and Windows 2003 are trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX<sup>(R)</sup> is a registered trademark of The Open Group in the United States and/or other countries.

HP-UX is a registered trademark of Hewlett-Packard Company in the United States and/or other countries.

Solaris is a registered trademark of Sun Microsystems., Inc. in the United States and/or other countries.

QwikScan is a trademark of NER data products inc. in the United States and/or other countries.

EDT-DistribuTAPE is a trademark of Gresham in the United States and/or other countries.

Other company, product, and service names may be trademarks or service marks of others.

# Contents

<b>INTRODUCTION TO AUTOVAULT .....</b>	<b>7</b>
<b>WHAT'S NEW IN AUTOVAULT VERSION 3.3.....</b>	<b>8</b>
Added support for TSM Version 5.5 and Version 6 .....	8
Added support for ActiveData pools.....	8
Vault copy pool media only when FULL.....	8
Checkpoint recovery of AutoVAULT from abnormal termination.....	8
Report media totals on reports and totals per vault location .....	8
Ability to run a post TSM Administrative Command .....	8
Automatically ftp media rotation reports to your vaulting company - Vital Records Inc® or Iron Mountain®.....	8
<b>WHAT'S NEW IN AUTOVAULT VERSION 3.0.....</b>	<b>9</b>
Added support for TSM Version 5.4.....	9
Manage Multiple TSM servers from one AutoVAULT install .....	9
Support for DRM functions and MOVE MEDIA command .....	9
Support for TSM Library Clients .....	9
New AutoVAULT execution PARM to automatically run multiple TSM servers .....	9
Remote Windows Server Management.....	9
Vault primary pool media only when FULL and/or by Last Reference Date .....	9
New AutoVAULT User Interface .....	10
External Software Interface Changes .....	10
Changes to Return media process for emergency onsite recovery .....	10
Added a media audit log .....	10
Font size parameter added for reports .....	10
<b>WHAT'S NEW IN AUTOVAULT VERSION 2.....</b>	<b>11</b>
Added support for TSM for Linux .....	11
Updated Report Formats .....	11
New Interface to QwikScan™ Media Manager .....	11
Ability to Reprint Reports.....	11
Support for Multiple Vault Locations .....	11
<b>AUTOVAULT V2 TO V3 UPGRADE CONSIDERATIONS .....</b>	<b>12</b>
<b>AUTOVAULT REQUIREMENTS .....</b>	<b>13</b>
Windows Workstation or Server .....	13
TSM Server for Windows, HP-UX, Solaris, Linux, or AIX .....	13
TSM administrative command line client .....	13
TSM Administrator access.....	13
FTP access for Remote Management.....	13
TSM ODBC Interface (TSM V5 or earlier) .....	14
TCP/IP connectivity to TSM server .....	14
<b>AUTOVAULT OVERVIEW.....</b>	<b>15</b>
How AutoVAULT works with Storage Manager .....	15
Disaster Recovery .....	15
Offsite storage of data.....	16

<b>INSTALLING, UPGRADING, AND CONFIGURING AUTOVAULT.....</b>	<b>17</b>
AutoVAULT Trial License .....	18
Multiple TSM Servers - Adding another TSM Server License Key .....	18
<b>Installation Checklist.....</b>	<b>20</b>
<b>Configuring AutoVAULT .....</b>	<b>21</b>
Specifying the AutoVAULT administrative ID and Password .....	22
Configuring the ODBC Data Source for AutoVAULT (TSM V5) .....	24
Configuring the Remote TSM Server .....	25
Selecting the Windows Server Instance .....	26
Choosing Copy Storage Pools for the vault .....	27
Choosing Primary and ActiveData Storage Pools for the vault .....	28
Selecting and configuring the libraries.....	30
Additional Settings.....	32
<b>AutoVAULT Management Console .....</b>	<b>34</b>
<b>AUTOVAULT OPERATIONS GUIDE .....</b>	<b>36</b>
Running or Scheduling AutoVAULT .....	36
Printing AutoVAULT reports .....	37
Emailing AutoVAULT Reports .....	38
Protecting AutoVAULT.....	38
Moving AutoVAULT.....	38
Creating Client Node Disaster Recovery Instructions.....	38
Returning Media from the Vault .....	40
Remote Access to AutoVAULT .....	41
QwikScan™ Interface.....	41
Checking in Media .....	41
Gresham EDT-Distributape .....	41
AutoVAULT Parameter Input.....	42
Running AutoVAULT Manually .....	43
Suppressing TSM Informational Messages.....	44
Audit Log - Tracking tape usage.....	44
Interface Files created by AutoVAULT.....	44
Automatically reporting to a Vaulting Company Like Vital Records Inc® or Iron Mountain®.....	45
Vault Location Changes.....	45
<b>DISASTER RECOVERY .....</b>	<b>46</b>
<b>Vaulting the Disaster Recovery Scripts.....</b>	<b>46</b>
<b>IBM Prepare Recovery Scripts.....</b>	<b>46</b>
<b>AutoVAULT Recovery Scripts.....</b>	<b>46</b>
Customizing the Disaster Recovery Scripts .....	46
Disaster Recovery Script Details.....	46
Disaster Recovery Instructions Example .....	47
<b>REFERENCE .....</b>	<b>51</b>
<b>AutoVAULT Options Reference: the vault.opt file.....</b>	<b>51</b>
<b>Audit Log Retention option: the AUDITLOG option.....</b>	<b>51</b>
<b>Backup Sets vault option: the BKSVault option.....</b>	<b>51</b>
<b>Specifying copypools to manage: the COPYPOOL option.....</b>	<b>51</b>
<b>Database backup vault option: the DBBVAULT option.....</b>	<b>51</b>

Database backup cycles to retain: the DBCYCLE option .....	52
Database snapshot backup cycles to retain: the DBSCYCLE option .....	52
Database snapshot backup vault option: the DBSVAULT option .....	52
Use DRM for media processing option: the DRMUSE option .....	53
Purging entries in the AutoVAULT log: the ERRLOG option .....	53
Report font size: the FONT option .....	53
Report FTP errors: the FTPERROR option .....	53
Using passive FTP: the FTPPASSIVE option .....	53
Selecting the Windows Server Instance: the ISERVER option .....	53
Defining libraries to AutoVAULT: the LIBRARY option .....	54
Running AutoVAULT in test mode: the MODE option .....	55
Check for vaulted media onsite: the ONSITECHK option .....	55
Specifying a command to run after AutoVAULT executes: the POSTCMD option .....	55
Specifying a command to run before AutoVAULT executes: the PRECMD option .....	56
Specifying primary and active data storage pools to move offsite: the PRIMARYPOOL option .....	56
Specifying report printing: the PRINTRPT option .....	56
Enabling the QwikScan™ Interface: the QWIKSCAN option .....	57
Specifying when to make returning tapes available: the REUSEDELAY option .....	57
Pull report heading: the RHPULL option .....	57
Return report heading: the RHRETURN option .....	57
Vault report heading: the RHVAULT option .....	57
Company report headings: the RPTHEAD option .....	58
Sorting the Reports: the RPTORDER option .....	58
Selecting which reports to print: the RPTSELECT option .....	58
Specifying level of security: the SECURITY option .....	58
Specifying TSM server FTP path: the SVFTPPATH option .....	58
Specifying TSM server Hostname or IP address: the SVIP option .....	59
Specifying TSM server Install path: the SVPATH option .....	59
Specifying TSM server DSMSEV_CONFIG path: the SVCPTH option .....	59
Specifying TSM server IP port: the SVPORT option .....	59
Specifying action on “tape in use” errors: the TINUSE option .....	59
Specifying a TSM Administrative command to run after AutoVAULT executes: the TSMPCMD option .....	59
Specifying which TSM version is being managed: the TSMVER option .....	60
Specifying verification of checkout process: the VCEDISABLE option .....	60
Specifying action on checkout errors: the VCHKOERR option .....	60
Specifying web reports: the WEBREPORT option .....	60
 Using the GBMAIL Client .....	 61
 <b>TROUBLESHOOTING</b> .....	 <b>62</b>
Error Messages .....	62
Known Problems .....	66
Technical Support .....	67
 <b>INDEX</b> .....	 <b>68</b>

# Introduction to **AutoVAULT**

**AutoVAULT is an enhancement to the Tivoli Storage Manager enterprise backup application for WINDOWS and UNIX servers.**

AutoVAULT intelligently manages and vaults all removable media containing TSM database backups, primary storage pool data, client backup sets, and copy storage pool data. You can choose between traditional vaulting and DRM vaulting. AutoVAULT creates disaster recovery instructions for you with all the necessary steps and scripts to restore your Storage Manager server environment in a minimal amount of time in addition to the prepare scripts created by DRM.

**AutoVAULT manages your critical backup data for you – every day.**

AutoVAULT automatically cycles critical Storage Manager backup data to one or more vault locations. Copies of your backup data and Storage Manager database backups are quickly identified for vaulting and items that are no longer needed in the vault are returned onsite.

**AutoVAULT ensures that the correct information is safely vaulted at all times with Media Rotation reports.**

AutoVAULT tells you which media to vault and which to return onsite. A report of your complete vault inventory is also created. All three of these reports can be emailed to one or more technicians, viewed through a browser, or automatically printed. By using AutoVAULT, you can feel secure about the status of your data from any location.

**Save time with an easy-to-use graphical interface to manage offsite media.**

Occasionally, offsite media must be brought onsite before it has expired to recover from an onsite media failure. With AutoVAULT, you select the desired volumes from an easy-to-use dialog. AutoVAULT excludes this media from normal operations and generates a report of volumes to return onsite. This allows you to continue normal vaulting operations while you recover.

**AutoVAULT allows you to vault TDP and archive data without copying it to a copy pool.**

AutoVAULT enables you to take your initial archives or TDP backups offsite, freeing expensive tape library slots and eliminating the time and media to duplicate the data to a copy pool. Using multiple vault locations, you can eject full primary pool media to an onsite vault location to free expensive library slots.

**Make your job easier, automate your Storage Manager disaster recovery with AutoVAULT.**

AutoVAULT creates disaster recovery instructions for you containing the necessary steps to restore your Storage Manager server environment in a minimal amount of time. Easy to use scripts will rebuild the Storage Manager server at your recovery site using the media AutoVAULT sent to the vault. The process is made easy to use so your staff can focus on other critical problems during a disaster. In addition, DRM prepare scripts are created and copied to a common name to allow for easy, automated offsite transfer.

# What's new in AutoVAULT Version 3.3

## Added support for TSM Version 5.5 and Version 6

Support has been added for changes introduced by version 5.5 of Tivoli Storage Manager (requires AutoVAULT v3.2 or higher) and version 6 of Tivoli Storage Manager (requires AutoVAULT v3.3.2 or higher). The TSM ODBC client is no longer required for TSM V6.

## Added support for ActiveData pools

Support for vaulting ActiveData pools has been added. This includes support for Library Clients.

## Vault copy pool media only when FULL

AutoVAULT can now restrict copy pool media vaulting to only eject FULL media. This allows you to remove a second copy pool version from your library only when the media is FULL, reducing the amount of unused tapes and reducing reclamation processes. This option should only be used in special situations. It is always best to remove offsite media quickly and not wait for the tape to become FULL.

## Checkpoint recovery of AutoVAULT from abnormal termination

AutoVAULT will recover from an abnormal termination and will not lose information about media movements prior to the failure.

## Report media totals on reports and totals per vault location

AutoVAULT will report media totals on all reports. If the report is sorted by vault location, a total will be printed for each location as well as a total for all locations.

## Ability to run a post TSM Administrative Command

AutoVAULT will run any TSM administrative command after processing your TSM server. This can also be a TSM server script containing several TSM administrative commands.

## Automatically ftp media rotation reports to your vaulting company - Vital Records Inc® or Iron Mountain®

AutoVAULT can ftp media reports to your vaulting company such as Vital Records Inc or Iron Mountain. AutoVAULT will automatically request media for return. It will also send the list of media sent offsite so the vaulting company can verify receipt. Your vaulting company will send you an error report if it does not receive the media.

# What's new in AutoVAULT Version 3.0

## Added support for TSM Version 5.4

Support has been added for changes introduced by versions 5.4 of Tivoli Storage Manager

## Manage Multiple TSM servers from one AutoVAULT install

One central AutoVAULT instance can manage multiple TSM servers running on different platforms. This allows you to simplify your TSM operations and quickly replicate configurations to a new TSM server instance. All AutoVAULT options are defined separately for each TSM server instance allowing maximum flexibility. An AutoVAULT license is required for each TSM server instance.

## Support for DRM functions and MOVE MEDIA command

AutoVAULT still supports the traditional vaulting method using CHECKOUT LIBV and UPDATE VOLUME commands, but now also supports all DRM functions including MOVE DRMEDIA, MOVE MEDIA, and PREPARE. You can choose which method works best for you for each TSM server instance.

## Support for TSM Library Clients

AutoVAULT supports TSM Library Clients using MOVE DRMEDIA and MOVE MEDIA commands. Backupset media management is not supported for a Library Client.

## New AutoVAULT execution PARM to automatically run multiple TSM servers

The AutoVAULT executable accepts parameter input to control which TSM server to execute when multiple TSM servers are defined. You can run one TSM server instance, all defined instances, or a combination of instances in any order. There is also a time delay option allowing a pause between executions. This allows you to run your TSM server, pause 30 minutes, and run the same server again. This is very useful when you are regularly exceeding your library I/O slots and need to run AutoVAULT multiple times.

## Remote Windows Server Management

AutoVAULT is no longer restricted to running directly on a TSM for Windows server. AutoVAULT will remotely manage a Windows server. FTP is required on the Windows server to access key TSM files.

## Vault primary pool media only when FULL and/or by Last Reference Date

AutoVAULT can now restrict primary pool media vaulting to only eject FULL media and/or media that has not been referenced for a specific number of days. Both options can be specified individually or combined. This allows you to remove long term data, such as archives, from your library when the media is FULL and vault it to an onsite vault location.

## **New AutoVAULT User Interface**

AutoVAULT functions have been combined into a single AutoVAULT management console allowing you to easily configure, execute, and administer your TSM servers from one location. If you manually execute AutoVAULT, a new GUI is provided which allows better control and the ability to enter parameter input.

## **External Software Interface Changes**

In addition to the combined interface file, AutoVAULT will also create separate tapeoff and tapeon interface files for each vault location. AutoVAULT will also create a unique interface file name for media returned for emergency use.

## **Changes to Return media process for emergency onsite recovery**

AutoVAULT will now exclude media brought onsite for an emergency. This allows you to continue normal vaulting operations while the media you need is left in your library. AutoVAULT no longer updates the status of your returned media. It creates a unique interface file so your media management software can handle the media differently

## **Added a media audit log**

AutoVAULT now maintains a log of all media changes. You can specify how many days the log data is retained. Older data is automatically deleted. The log is in CSV format for easy reporting from Excel or other products.

## **Font size parameter added for reports**

AutoVAULT accepts a new FONT parameter in the vault.opt file so you can change the default font size. You can also change the page orientation from portrait to landscape by changing the attributes of your default printer. Using these two options, you can change the report size to be larger or smaller.

# What's new in AutoVAULT Version 2

## Added support for TSM for Linux

Support has been added for TSM running on Linux x86 or pseries.

## Updated Report Formats

The format of the three vaulting reports has been changed. The legacy AutoVAULT report format is still available. The new format allows each of the three reports to be sorted separately on multiple values. A new RPTORDER option has been added to specify the report order for each report. New options have been added to change the default report title on each of the reports. The RHPULL, RHRETURN, and RHVAULT options allow you to override each report title or use the AutoVAULT default.

## New Interface to QwikScan™ Media Manager

We have teamed up with a leading media management product, QwikScan, to bring AutoVAULT customers additional functionality including the ability to track media by Barcode ID and manage random slot vaulting. AutoVAULT has been improved to work seamlessly with QwikScan by automatically updating QwikScan with media changes initiated by AutoVAULT. QwikScan is an affordable, Windows based media manager product from NER Data Products, Inc. for mainframe, midrange and distributed environments. For more product information and pricing, please visit <http://www.nerdata.com/>.

## Ability to Reprint Reports

A new feature has been added to allow reprints of any of AutoVAULT's reports to any defined printer.

## Support for Multiple Vault Locations

You can now specify different vault locations for all media including TSM database backups (both regular and snapshot), backupsets, copy pools, and primary pools. Each copy pool and primary pool can have a different vault location. By sorting your vault reports on vault location, separate vaulting reports will be created to allow separate reporting to each individual vault. This feature allows you to easily maintain a set of media in both an onsite and an offsite vault.

# AutoVAULT V2 to V3 Upgrade Considerations

AutoVAULT can be upgraded from V2 to V3 with only minor changes. As with any AutoVAULT upgrade, you should run the configuration wizard for your TSM server instance. The wizard will make any necessary changes to your configuration settings.

- If you define more than one TSM server instance to AutoVAULT, then you **MUST** pass a parameter to the AutoVAULT executable (autovault.exe). If you execute manually, this parameter is supplied for you. If you execute AutoVAULT from a TSM or command script, then this will cause you an error. You should use the provided command file to execute your TSM server instance. Refer to section “Running or Scheduling AutoVAULT” in this manual for details.

- If you are using the QwikScan interface to pass files to external software, you will need to add the new return media file. Tapes brought onsite prematurely for an emergency onsite restore will be included in an interface filename beginning with “tapeon\_restore”.

- If you decide to change between vaulting methods, you may see vaulted media on the first pull report. The two vaulting methods track media in different ways and the first execution with the new method will “catch up” and may vault some of your TSM database backup volumes again.

# AutoVAULT Requirements

## Windows Workstation or Server

AutoVAULT runs on Windows. It can be run on the TSM for Windows Server or from a remote Windows workstation or server. AutoVAULT has been tested with 2000 Pro, XP, Vista, 2000 Server, and 2003 Server. AutoVAULT can run as a VMware guest running on any supported Windows operating system. Note that Windows x64 is not supported at this time.

## TSM Server for Windows, HP-UX, Solaris, Linux, or AIX

AutoVAULT will manage Tivoli Storage Manager (TSM) versions 5.1 through 5.5. TSM must be running on a Windows, AIX, HP-UX, Linux, or Solaris platform. To manage a TSM server, AutoVAULT must run on a Windows server or workstation with TCP/IP access to the TSM server. The TSM administrative command line client, the TSM ODBC interface, and FTP are used by AutoVAULT to remotely manage the Storage Manager Server and you must have at least one volume history file and device configuration file defined at the same location as the DSMSEV.OPT file.

## TSM administrative command line client

A TSM administrative command line client is required for the operation of AutoVAULT. AutoVAULT supports the TSM Windows client versions 5.1 through 5.5. You should install a version that matches the version of your TSM Server. The TSM administrative client must be installed on the same Windows server or workstation running AutoVAULT. The TSM administrative client is bundled with the TSM backup/archive client and must be installed using a custom install.

Download here: <ftp://ftp.software.ibm.com/storage/tivoli-storage-management/>

## TSM Administrator access

AutoVAULT requires a TSM administrator with system privilege so that it can communicate with the Storage Manager server. After the userid and password are supplied and verified during the AutoVAULT installation, they are encrypted for AutoVAULT to use when it runs. If the userid and/or password need to be changed at a later date, run AutoVAULT configuration by selecting 'Configure' from the AutoVAULT management console.

## FTP access for Remote Management

If AutoVAULT is managing a TSM server remotely, a userid is required with ftp access (active or passive) to the Storage Manager server's configuration files. After the userid and password are supplied and verified during the AutoVAULT installation, they are encrypted for AutoVAULT to use when it runs. If the userid and/or password need to be changed at a later date, run AutoVAULT configuration by selecting 'Configure' from the AutoVAULT management console. On TSM for Windows, you must enable the FTP server and create a virtual ftp directory to the location containing your dsmserv.opt file.

## TSM ODBC Interface (TSM V5 or earlier)

The TSM ODBC interface must be installed and configured for AutoVAULT to function correctly with TSM Server versions prior to TSM V6. The TSM ODBC client was eliminated with TSM V6 and the IBM DB2 ODBC client is not used by AutoVAULT for TSM V6 Servers. The TSM V5 ODBC interface is bundled as a separate install from the TSM backup/archive client.

Download here: <ftp://ftp.software.ibm.com/storage/tivoli-storage-management/>

## TCP/IP connectivity to TSM server

The ODBC interface, TSM administrative client, and FTP require TCP/IP access to the Storage Manager server. If your TSM server runs remotely, the server or workstation running AutoVAULT must have TCP/IP communications to the TSM Server.

# AutoVAULT Overview

## How AutoVAULT works with Storage Manager

AutoVAULT communicates with the Storage Manager server to vault copy storage pool volumes, primary storage pool volumes, Storage Manager database backup volumes, and Backup Set volumes based on your selections. Each media type can be assigned the same or different vault locations. Any volumes in the managed pools that are either full or filling when AutoVAULT runs, are checked out of the library to be sent to your vault location. You can restrict the vaulting of primary pool media to those FULL or unreferenced for a specific number of days. You can restrict the vaulting of copy pool media to only those FULL, although this is not recommended in most circumstances. Similarly, any database backup volumes or backup set volumes in the library at the time that AutoVAULT runs are checked out of the library to be sent offsite. Note that backupset media is not supported for a TSM Library Client. Once empty, volumes ready to return from offsite storage are updated and reported in the list of volumes to return onsite.

## Disaster Recovery

The term “Disaster Recovery” specifically refers to a situation where you have lost your data. Two scenarios that fall under this heading are:

- Physical damage to a branch office through fire, flood, or some other natural or man-made disaster, making it necessary to set up a temporary facility. This would most likely involve re-creation of local servers and the restoration of the data needed on those servers. As ugly as this scenario is, it would probably not require access to offsite copies of backed-up data, unless there is a problem with the media of the backups available onsite with the Storage Manager server.
- Physical damage to a central office including damage to or destruction of the Storage Manager server. This scenario would require reinstallation of Storage Manager on a new server and restoration of the Storage Manager database from backup volumes before other servers can be restored. Almost certainly, offsite copies of backed-up data would be required, unless the libraries were somehow spared from the destruction. Obviously, this is a much more serious type of disaster.

While recovering from a total data loss is almost guaranteed to require a valid set of offsite media, recovery from other situations can be made possible by bringing offsite media back.

- Database corruption or destruction. The Storage Manager database could get corrupted or destroyed. In the case of corruption, if the problem is not discovered immediately, having a number of database backups available allows you to recover the database to a prior working state.
- Media problems with onsite volumes. Fixed and removable volumes can both experience failures resulting from mishandling or hardware failure. Having media available offsite gives you the opportunity to recover from media failures and reconstruct the onsite primary storage pools.

## Offsite storage of data

Backup media should be moved to a secure remote site as frequently as is practical. Arranging to have a courier arrive daily to transport the media offsite is **not** overkill. This kind of service can be surprisingly inexpensive. AutoVAULT will assist you in accurately identifying all of the volumes to be taken offsite after the regularly scheduled database and storage pool backups are completed.

AutoVAULT takes the following approach to media rotation:

- For Storage Manger database backups that AutoVAULT is configured to manage, volumes that are not in the vault are checked out of the library and listed on a report to be taken offsite.
- For each copy storage pool that AutoVAULT is configured to manage, volumes that are available locally and contain data are checked out of the library. With traditional vaulting, the access parameter of the volume is then set to OFFSITE. With DRM vaulting, the MOVE DRMEDIA command is used to update the volume status. The volume is listed on the report of tapes to go offsite.
- For each primary storage pool that AutoVAULT is configured to manage, volumes that are available locally and contain data are checked out of the library. With traditional vaulting, the access parameter of the volume is then set to UNAVAIL. With DRM vaulting, the MOVE MEDIA command is used to update the volume status. The volume is listed on the report of tapes to go offsite
- If AutoVAULT is configured to manage backup sets, volumes that are not in the vault are checked out of the library and listed on a report to be taken offsite. Neither MOVE MEDIA nor MOVE DRMEDIA commands support backupsets, so a CHECKOUT LIBVOLUME command is used.
- If you do not want AutoVAULT to expire your Storage Manager database volumes, you can configure it to only cycle database volumes offsite by setting the database cycle option to zero and selecting yes for the vaulting option.

If AutoVAULT is configured to expire database volumes, the following is true:

### Traditional Vaulting Method

- Any volumes belonging to a database backup series in excess of the specified cycle retention are scratched.
- AutoVAULT will always retain at least one database backup series, no matter how old. An old database backup is better than none.
- Any volumes scratched by deleting volume history are listed on the report of tapes to return onsite, and they become available for reuse.

### DRM Vaulting Method

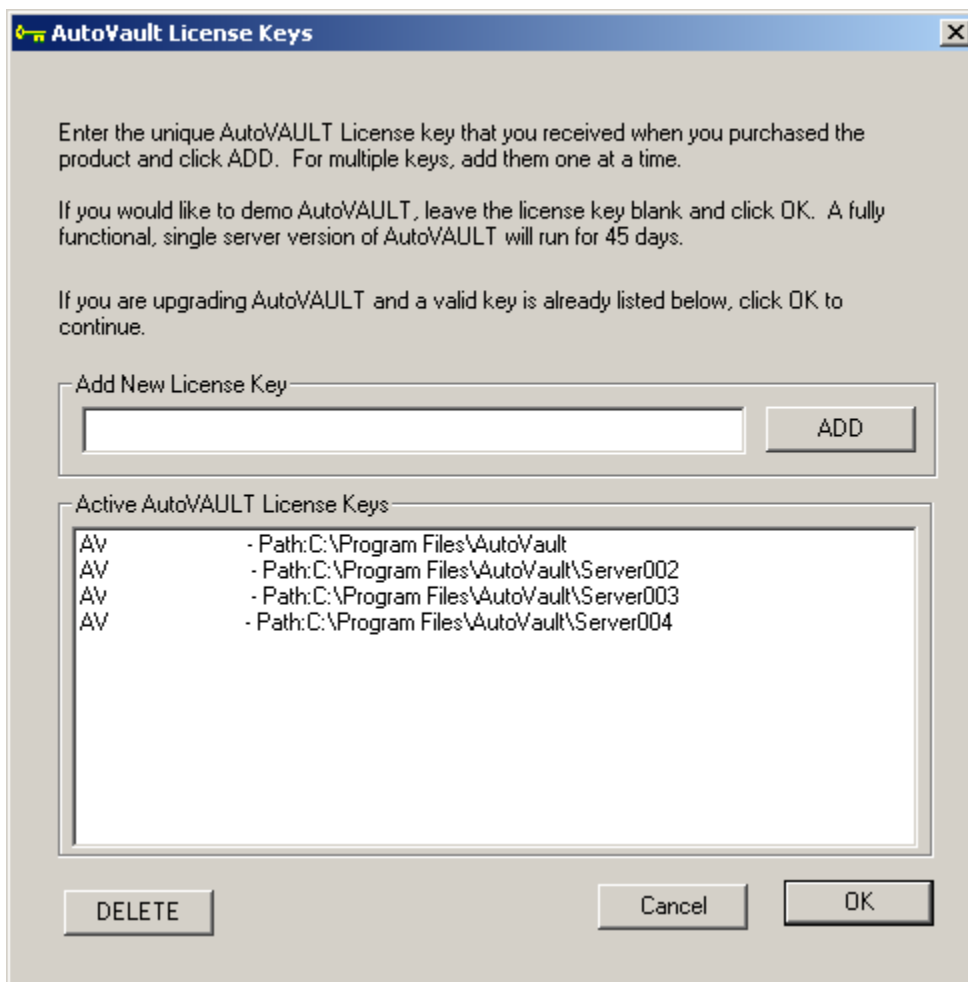
AutoVAULT sets the DRMDBBACKUPEXPIREDAYS value to the highest value specified for TSM database or snapshot backups. DRM uses one global value for both TSM database backup types.

# Installing, Upgrading, and Configuring AutoVAULT

AutoVAULT is installed or upgraded by running setup.exe from the install media or the location where you downloaded it. Setup.exe is a self-extracting install; no additional files are required. There is no need to uninstall a previous or demo version of AutoVAULT before upgrading. The installation process requires the following pieces of information to complete:

1. Where do you want to install the program?
2. What Program Folder should the AutoVAULT icons be created in?
3. What is your AutoVAULT license key? Leave this blank for a 45 day trial.

During the installation, you will be asked to verify your AutoVAULT license key.



Installation will not continue if you do not have a valid license key with current maintenance. If this is a first time install, you can leave the license field blank for a 45-day trial demo.

## AutoVAULT Trial License

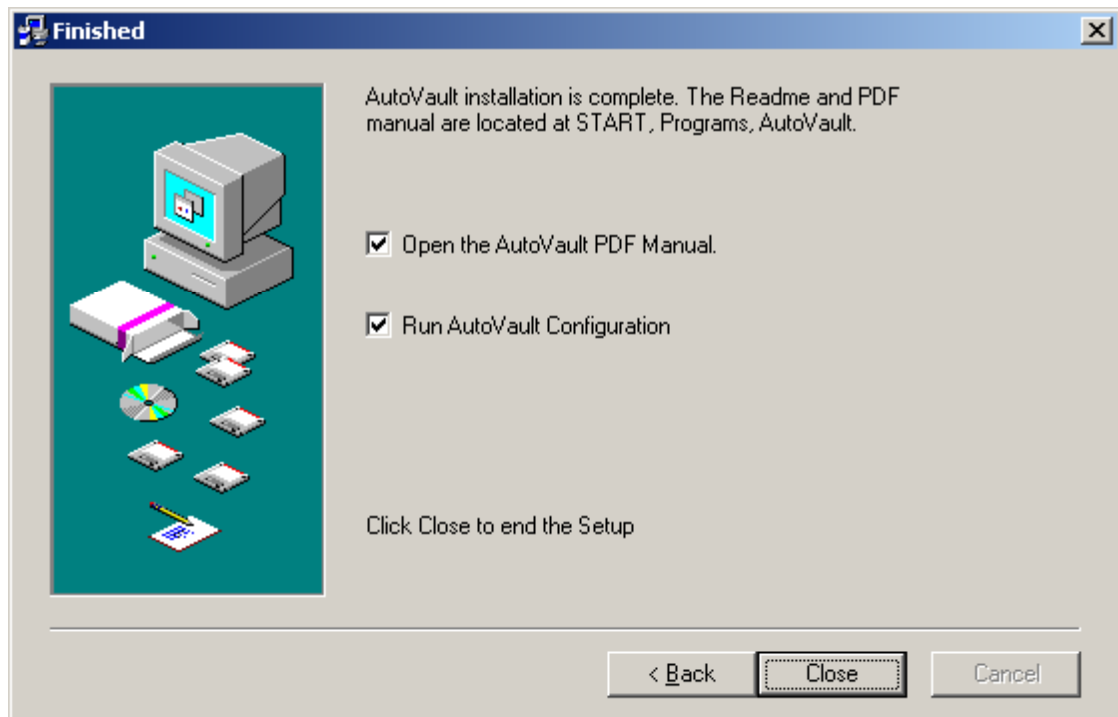
You can run a 45-day trial of AutoVAULT only if you have not previously entered a permanent license key. The trial license will only allow one TSM Server definition. There is no trial license for managing multiple TSM Servers. This is a full function license allowing use of all the AutoVAULT features and functions. Note that you have the option during configuration to run AutoVAULT in demo mode so that none of your TSM media is updated or moved. This is an excellent way to trial AutoVAULT and see all the rich features and benefits of the product without affecting your TSM Server.

## Multiple TSM Servers - Adding another TSM Server License Key

If you have already installed and configured one AutoVAULT license and TSM server, you can purchase additional AutoVAULT licenses to manage more TSM servers. You need one AutoVAULT license per TSM Server. To add additional AutoVAULT licenses, run “AutoVAULT License Key” from the AutoVAULT Program Group. On the AutoVAULT License Key screen, enter your new license key in the “Add New License Key” field and click “Add”. Your new license key will appear in the “Active AutoVAULT License Keys” window” along with the unique directory path that was created for this TSM Server instance. Each TSM Server managed by AutoVAULT uses a different subdirectory in the AutoVAULT installation folder. After you have added your new license key, click “OK” to close the license window and select “Manage AutoVAULT” from the AutoVAULT program group to start the AutoVAULT Management Console. Highlight your new license key and run configuration by clicking “Configure”.

If you are installing or upgrading AutoVAULT, Click OK to continue with the installation. An important notices dialog will display next.

After all of the installation tasks are completed, you will see the following dialog:



Here you have the chance to configure AutoVAULT for operation immediately after Setup completes. We recommend checking both boxes so you can install AutoVAULT and have it configured and operational in under five minutes. The AutoVAULT Management Console will start. Highlight your TSM server instance and click “Configure” to start the configuration wizard.

If you are upgrading an existing version of AutoVAULT, run Configuration for each TSM server instance you are managing.

After you finish the configuration, all that remains to be done is the scheduling of AutoVAULT.

## ***Installation Checklist***

- Review the AutoVAULT installation requirements. Your Storage Manager server should be running on Windows, HP-UX, Solaris, Linux or AIX. The Windows workstation or server that you plan to run AutoVAULT on must have the Storage Manager administrative command line client and the Storage Manager ODBC interface (TSM V5 only) installed. Run the TSM administrative command line client and login using the userid you plan to use with AutoVAULT to verify it is working properly.
- Verify that your Storage Manager Server has a device configuration file and a volume history file defined in the same location as your DSMSEV.OPT file. Refer to the Storage Manager Administrative reference manual for details on defining these.
- Install AutoVAULT and follow the configuration instructions in this manual, section 'Configuring AutoVAULT'
- You can run AutoVAULT manually by selecting "Run AutoVAULT" from the AutoVAULT Management Console.
- It is preferable to automate the daily execution of AutoVAULT using the Storage Manager Scheduler. Install the Tivoli Backup/Archive client on the Windows workstation or server that you plan to run AutoVAULT on. Using Services in the Windows Control Panel, setup the TSM Scheduler Service to run under a userid with access to your default printer. Be sure this userid also has the right level of security so that you can run daily backups of this workstation or server.
- Create a Storage Manager Server script to create your disaster recovery media and automatically execute AutoVAULT. Refer to the "Running or Scheduling AutoVAULT" section in this manual for more details and a sample script.
- Ensure that the Disaster Recovery scripts are taken offsite every time you run AutoVAULT. One option is to copy them to a floppy disk, CD, or DVD for vaulting. Refer to sample script "Copyscript\_bat.smp" in the AutoVAULT install directory for details. Another option is to ftp the files automatically to a remote site every time AutoVAULT runs. Refer to sample script "avpost\_cmd.smp" in the AutoVAULT install directory for details.
- Setup email of the AutoVAULT media reports. This can be run as a POSTCMD every time AutoVAULT runs. Refer to sample script "avpost\_cmd.smp" in the AutoVAULT install directory for details.

## **Configuring AutoVAULT**

AutoVAULT provides a graphical interface to configure almost all aspects of its operation. You can choose to configure it immediately after installing AutoVAULT, when you are prompted during the installation. You can also run it at a later time by clicking “Configure” from the AutoVAULT Management Console.

You must use the AutoVAULT configuration program before it will be operational. This process encrypts and stores the administrative password for future use by AutoVAULT. If you attempt to run AutoVAULT without first running the configuration program, it will fail. After running the configuration program, you can manually edit the **vault.opt** file to make any changes that might be required or click “Configure” from the AutoVAULT Management Console again.

There are additional benefits to running the configuration program. As you fill in the fields and progress through the dialogs, the ODBC Data Source used for querying the server is created. At that point, AutoVAULT then uses the ODBC interface to extract the information you need to configure the management of your storage pools and libraries. When the configuration program completes, it writes the vault.opt file, and you have a working AutoVAULT configuration. The few AutoVAULT options that it does not configure are explained in the section [AutoVault Options Reference: the vault.opt file](#).

The following sections show the dialogs that appear when running the configuration program and explain the various settings available.

## Specifying the AutoVAULT administrative ID and Password

**TSM Server Definition**

TSM Administrator: admin

TSM Password: \*\*\*\*\*

Re-enter Password: \*\*\*\*\*

TSM Server Address: tsmsserver

TSM Server Port: 1500

AutoVAULT is running on the selected TSM Server

Use Disaster Recovery Manager functions (DRM)

TSM Version 6 Server

User defined name for the TSM Server instance. MUST be alphanumeric, without spaces or special characters.

MAINOFFICE

Run in READONLY, TEST mode with no TSM updates

For help in configuring AutoVAULT, refer to the AutoVAULT manual which is available from the AutoVAULT Program Group or online at <http://www.codereleief.com/avmanual.htm>

< Back   Next >   Cancel

**TSM Administrator and password** - used by AutoVAULT for queries and checking out the volumes to be sent to the vault. The administrator must have system privilege.

It is a good idea to create a distinct TSM administrative userid for the vaulting process; this separates the vaulting process from specific personnel. If the ID belongs to an administrator who gets reassigned to other duties in the future and their ID is disabled or deleted, offsite processing will not run.

**TSM Server Address and Server Port** - The default port number is 1500. The server address can either be a hostname or an IP address, provided the hostname can be resolved to an IP address.

**AutoVAULT is running on the TSM for Windows server** - Check the box if you are running AutoVAULT on a TSM for Windows server. Otherwise, leave the box unchecked.

**Use Disaster Recovery Manager functions (DRM):**

**DRM Vaulting Method** - Check the box

AutoVAULT will use MOVE DRMEDIA and MOVE MEDIA commands to update media. TSM database backups will be expired by date using the DRM DRMDBBACKUPEXPIREDAYS setting. PREPARE files will be created for both DBB and DBS database backups. Traditional AutoVAULT recovery scripts will still be created. You must have a TSM Extended server license from IBM to use this option. You must select this option for TSM Library Client.

**Traditional Vaulting Method** - Uncheck the box

AutoVAULT will use CHECKOUT LIBV and UPDATE VOLUME commands to update media. TSM database backups will be managed by cycles instead of date. You cannot use this method with TSM Library Clients. This method is for any TSM server license, Base or Extended.

**TSM Version 6 Server:** If you are managing a TSM V6 Server, check this box. You will not be asked to confirm an ODBC connection. All interaction with a TSM V6 Server is through the TSM Administrative Client.

**User Defined name** - Define a name for this TSM server instance. If you are managing multiple TSM servers from AutoVAULT, this will help you identify which server you are managing. This value can also be passed to AutoVAULT as an execution parameter.

**Run in READONLY Test Mode with no TSM updates** - If you would like to test AutoVAULT and not have it update your TSM server, check this option. You can configure and run AutoVAULT against your TSM server without changing your TSM server. Note that some of the report output will not be correct for multiple executions since AutoVAULT did not actually change the status of your media. This is a very good way to try AutoVAULT during your trial period.

## Configuring the ODBC Data Source for AutoVAULT (TSM V5)

The screenshot shows a dialog box titled "Configure a TSM Data Source". It contains the following fields and options:

- Data source name: AutoVault ADSM Data Source
- Description: (empty)
- Language: English (US)
- Administrator name: (empty)
- Fetch size: 500
- TSM server connection:
  - TCP/IP address: 172.30.80.109
  - TCP/IP port: 1500
- Tracing:
  - Enable trace.
  - Trace file name: odbcadsm.trc

At the bottom of the dialog are "OK" and "Cancel" buttons.

Do not change the Data Source Name (DSN). The DSN is created as a System Data Source so that it will always be available as long as the machine is running (even from a Windows service). For a performance gain, increase the "Fetch size" to 1000 and do not enable tracing.

## Configuring the Remote TSM Server

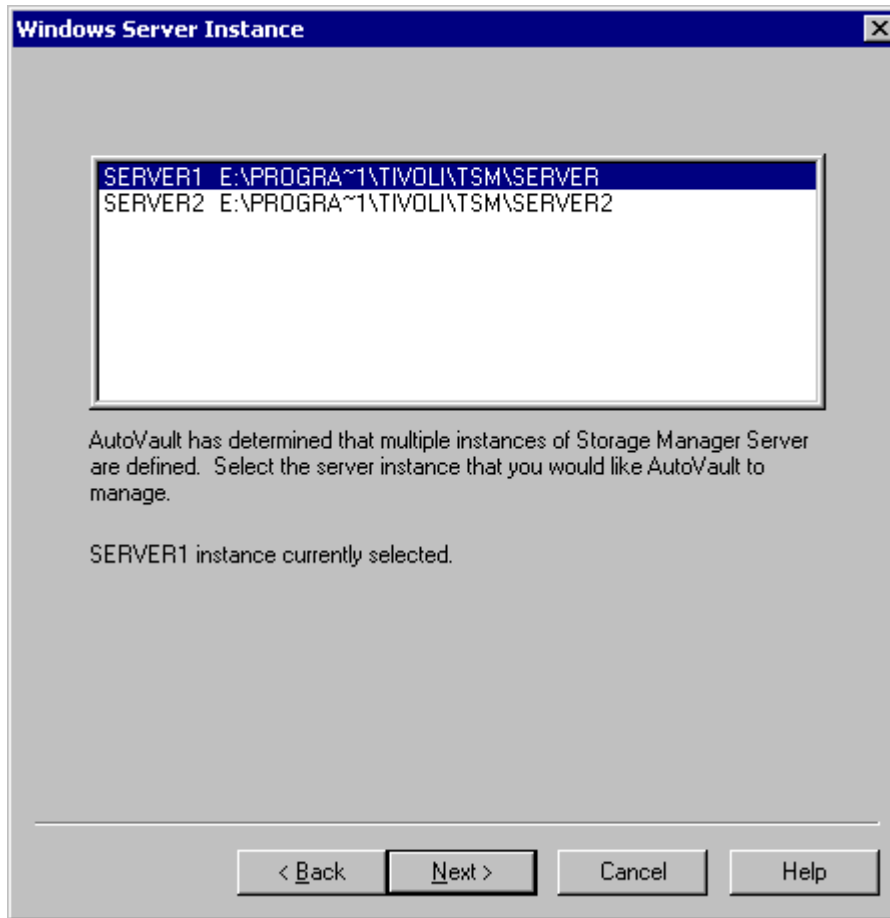
The screenshot shows a Windows-style dialog box titled "Remote TSM Server". At the top, a message box states: "Your Tivoli Storage Manager Server is running on a remote server. Please enter the following to allow for the FTP of key server data used by the recovery scripts." Below this, there are several input fields and checkboxes:

- FTP userid:** A text box containing "administrator".
- FTP password:** A text box containing "\*\*\*\*\*".
- Re-enter password:** A text box containing "\*\*\*\*\*".
- Storage Manager install path (DSMSERV\_DIR):** A text box containing "c:\progra~1\Tivoli\TSM\server".
- Storage Manager Server Instance path (DSMSERV\_CONFIG):** A text box containing "c:\progra~1\Tivoli\TSM\server".
- FTP Server Virtual Directory Path (TSM for Windows only):** A text box containing "tsm\".
- Use Passive FTP:** An unchecked checkbox.
- Verify FTP Values:** A checked checkbox.

At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

If you indicated that AutoVAULT is not running on the TSM server, you will be prompted to supply TSM installation and FTP information. Supply a userid and password that has FTP access to the Storage Manager server's option file (DSMSERV.OPT), volume history backup files, and device configuration backup files (all in the same directory). You must also supply the path on the TSM server where you installed Storage Manager and the path that contains the server option file, DSMSERV.OPT. If you are remotely managing TSM for Windows, you will need to enable an FTP server and create a virtual directory path. Supply the FTP virtual path to AutoVAULT. AutoVAULT will verify that all of these values are valid if you check the box "Verify FTP Values" (recommended). Check the box "Use Passive FTP" if you prefer this FTP method. The userid and the password are encrypted.

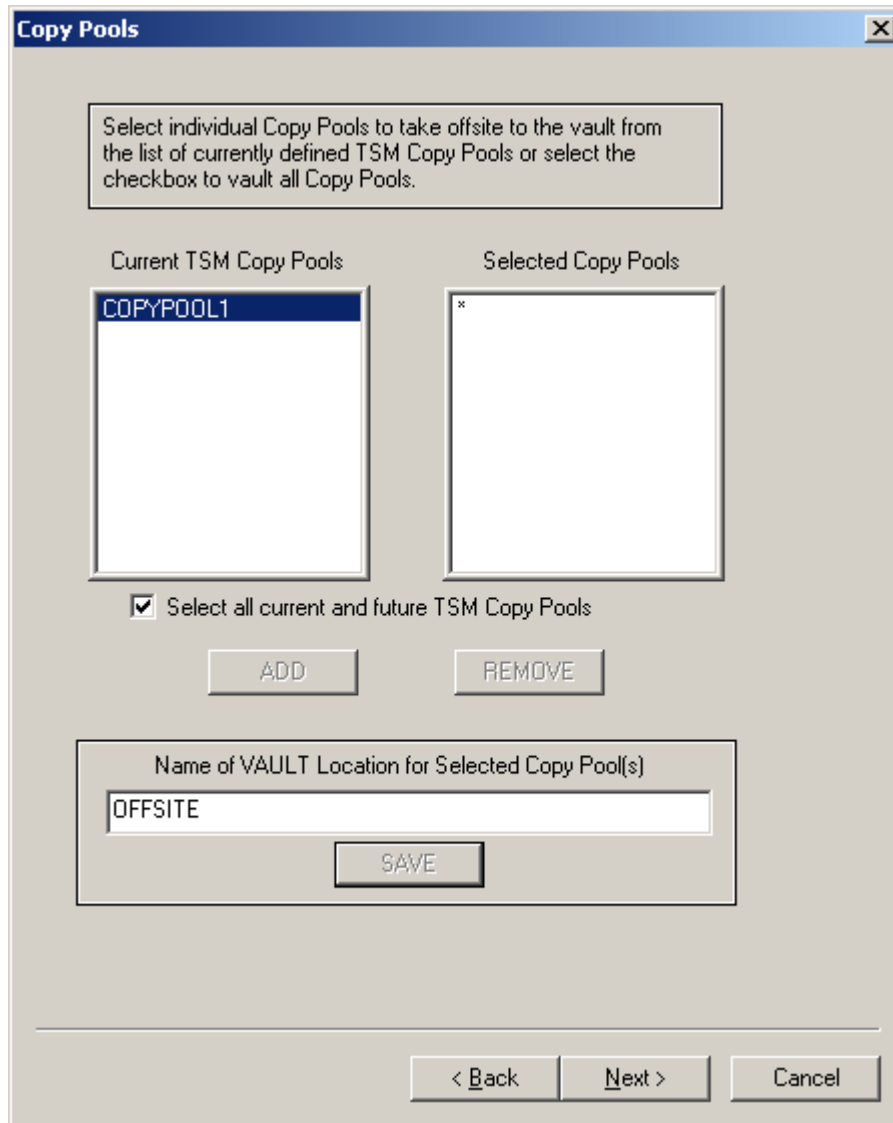
## Selecting the Windows Server Instance



If you indicated that AutoVAULT is running on the TSM server and multiple Storage Manager Servers have been created, you will be prompted to select which Storage Manager instance AutoVAULT should manage. AutoVAULT can manage only one server instance per AutoVAULT license. If you only have one Storage Manager instance defined, this screen will not be displayed.

Highlight the correct Storage Manager server instance to select it.

## Choosing Copy Storage Pools for the vault

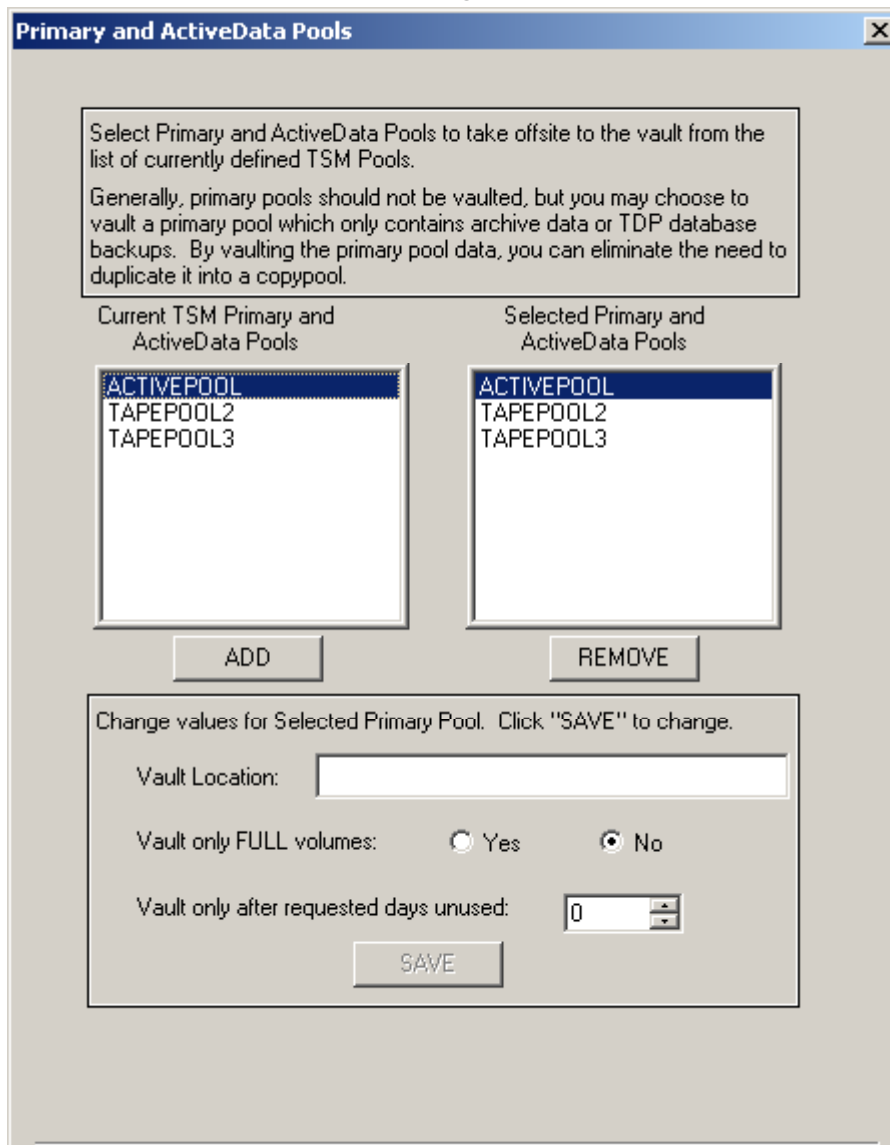


In this dialog, select the copy pools that you want to maintain in the vault. Frequently, you will want all cospools sent offsite to the vault. If this is the case, select the “Select all current and future TSM Copy Pools” checkbox.

If you have onsite copy pools that need to stay in the library, clear the checkbox, highlight the copy pools that need to be vaulted, and click ADD. If you decide to stop vaulting a copy pool or select a copy pool in error, highlight the cospool in the pane on the right and click REMOVE.

You can send cospool media to different vault locations. Highlight a cospool under “Selected Copy Pools”, enter a vault location, and click SAVE. You can also change the name of the vault location the same way. If you checked the box for all copy pools, then the vault location will be applied to all copy pool media. You must click “SAVE” to make a change before leaving this screen.

## Choosing Primary and ActiveData Storage Pools for the vault



Select any primary and activedata pools that you would like to maintain in the vault. Offsite relocation of primary storage pool volumes is a feature of AutoVAULT that allows you to make better use of your library capacity. Storage Manager considers all primary storage pools to be local and readily available, which for most circumstances makes perfect sense. But what if the data stored in one or more of your primary pools is very static, referenced infrequently, and has long retention periods?

You might encounter such a scenario if your service level agreements require quarterly or yearly archives of critical clients, all of which need to be retained for several years. You may also want to avoid duplicating the database backups created by Tivoli Data Protection agents. Simply direct your TDP backups to a separate primary tape pool and use AutoVAULT to send them to the vault. The tapes are removed from your library freeing expensive slots. You also avoid the time consuming task of copying the data to a copy pool.

Highlight the primary and activedata pools that you wish to vault, and click ADD. If you decide to stop vaulting a pool, or selected a pool in error, highlight the pool in the pane on the right and click REMOVE.

You can send primary and activedata pool media to different vault locations. Highlight a pool under “Selected Primary and ActiveData Pools”, enter a vault location, and click SAVE. You can also change the name of the vault location the same way. Use this feature to vault primary pools with a long retention period to an onsite vault location.

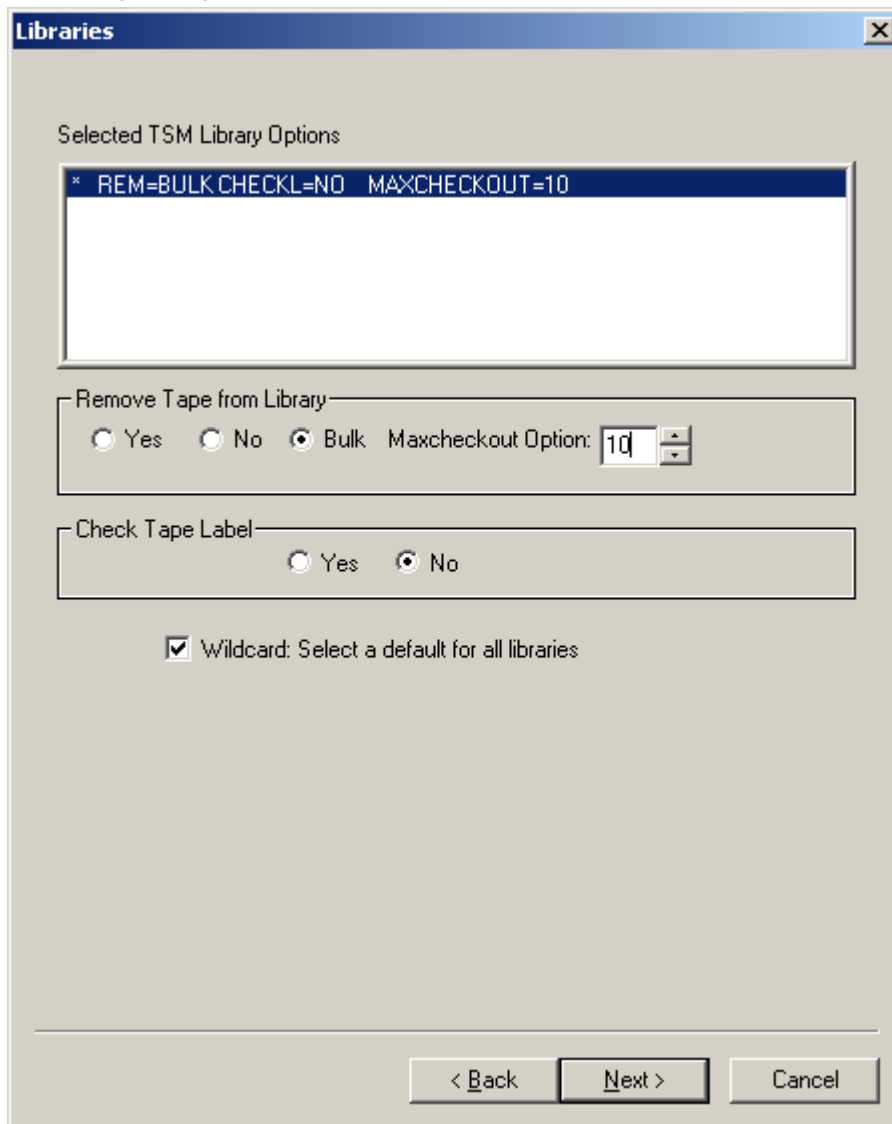
You can direct AutoVAULT to only remove the primary or activedata pool volume if it is FULL. Select ‘Yes’ and AutoVAULT will only vault a volume for this pool when it is FULL.

You can direct AutoVAULT to only remove the primary or activedata pool volume if it has not been read or written in a specified number of days. AutoVAULT will only vault a volume from this pool when it has not been referenced for the requested number of days.

If you specify both a FULL volume restriction and an unused number of days, then AutoVAULT will only vault a volume from this pool when both criteria are met.

You must click “SAVE” to make a change before leaving this screen.

## Selecting and configuring the libraries



Select the checkout options for each tape library. This option only applies to automated libraries. By default, the wildcard option (to select a default for all libraries) is selected and your choices apply to all current and future libraries. If you clear the wildcard option, all your currently defined libraries will be displayed. You can then select different options for each individual library by selecting the appropriate REMOVE and CHECKLABEL options.

For automated libraries with multiple input/output ports, you can specify the BULK option so that volumes are ejected to the I/O ports until the value of MAXCHECKOUT is reached. AutoVAULT assumes the number of I/O ports you select are available and will continue to eject media until those slots are full. If more media must be ejected than the selected number of I/O ports, then AutoVAULT will issue an error message and will not vault the remaining media. You should empty the I/O ports and run AutoVAULT again to vault the remaining media.

Setting the MAXCHECKOUT value to '0' disables this option. If set to '0', AutoVAULT will fill all the I/O ports. If more media must be ejected than the number of physical I/O ports, then you must manually eject the media from the tape library.

## Database and Backup Set Options

**Database Backup Expiration**

Define how many Database Backups to retain. If you are using DRM, the value is the number of days to retain backups. If you are not using DRM, the value is the number of cycles to retain.

A value of '0' disables the deletion of Database Backup tapes. You can specify different deletion criteria for Full/Incremental and Snapshot backups only if you are not using DRM. For DRM, the largest value is used.

Database Full and Incremental Backup Retention: 3

Database Snapshot Backup Retention: 3

**Vault Properties**

Vault Full and Incremental Database Backups?  Yes  No  
VAULT Location VAULT2

Vault Snapshot Database Backups?  Yes  No  
VAULT Location VAULT3

Vault Client Backup Sets?  Yes  No  
VAULT Location

< Back Next > Cancel

**Database Backup Expiration with Traditional Vaulting** – Select the number of Storage Manager database backup cycles to retain. A full database backup and all the subsequent incremental backups are considered one cycle. For database snap backups, each backup is a full backup and is considered a cycle. Older versions will be deleted and returned onsite, if applicable.

**Database Backup Expiration with DRM** – If you are using DRM vaulting, then the highest database retention value will be used to set the DRMDBBACKUPEXPIREDAYS setting which controls the number of days to retain TSM DB backups. These are deleted during TSM EXPIRE processing.

To turn off AutoVAULT expiration of database backup volumes, select '0'. These values are also used to determine how many versions of the disaster recovery scripts are retained. The larger of the two values is used. A minimum of two backup copies of the disaster recovery scripts will always be retained.

**Vault Properties** - Select whether you want to vault each data type. Vaulting criteria is set independently of the expiration criteria. If you select 'Yes', Storage Manager database backups and/or backup sets will be included in the offsite vaulting reports. Vaulted volumes will be returned onsite when they expire. Enter the name of the vault location for each media type as needed.

## Additional Settings

**Additional Settings**

Report Settings

Headings

Company	Code Relief LLC
Pull Report	
Return Report	
Vault Report	

Print reports to the default Printer?  Yes  No

Create Reports in Server Scripts?  Yes  No

Sort Order: Double click sort criteria to move it up in the order.

Tapes Offsite	Tapes Onsite	Tape Inventory
VAULT	VAULT	VAULT
LIBRARY	VOLSER	TYPE
VOLSER	TYPE	POOL
TYPE		VOLSER

Use AutoVAULT Legacy report format

Level of Security:  High  Low

Vault Volume on Checkout Error:  Yes  No

Returning Volume Reuse Delay: 0

Pre-Command:

Post-Command:

TSM Post Cmd:

< Back Finish Cancel

**Report Headings** – For “Company”, enter the report heading that will appear on all your AutoVAULT reports. You can also override the default report heading on each of the three reports by filling in your own heading. If you leave the Pull, Return, or Vault report headings blank, then the default heading will be used.

**Print Reports** - Select whether AutoVAULT reports should be printed to the default printer. If you are running AutoVAULT automatically using the Storage Manager Scheduler Service, you will need to run the service under a user with a default printer assigned. The Windows system account does not have a default printer. If you would like reports printed, you must run the Storage Manager scheduler from a userid with a default printer defined.

**Reports in Server Script** - Select whether AutoVAULT media reports should be created as Storage Manager Scripts so they can be viewed from the TSM web interface. If you have a large amount of offsite media, selecting 'NO' will reduce the amount of Storage Manager Server activity log entries created when AutoVAULT runs.

**Report Format** – A new report format was introduced with AutoVAULT v2.0. If you prefer to use the old format, check the box for “legacy report format”. Uncheck the box to use the new format. With the new format, you can sort the individual reports using the displayed criteria. Reports are sorted in the order you select from the top down. Double click a sort criteria to move it up in the sort order.

**Security Level** – Select the level of security for AutoVAULT processing. If low security is selected, the administrator and userid will be included in the disaster recovery scripts. If high security is selected, you will need to provide a valid administrator and password at disaster recovery time.

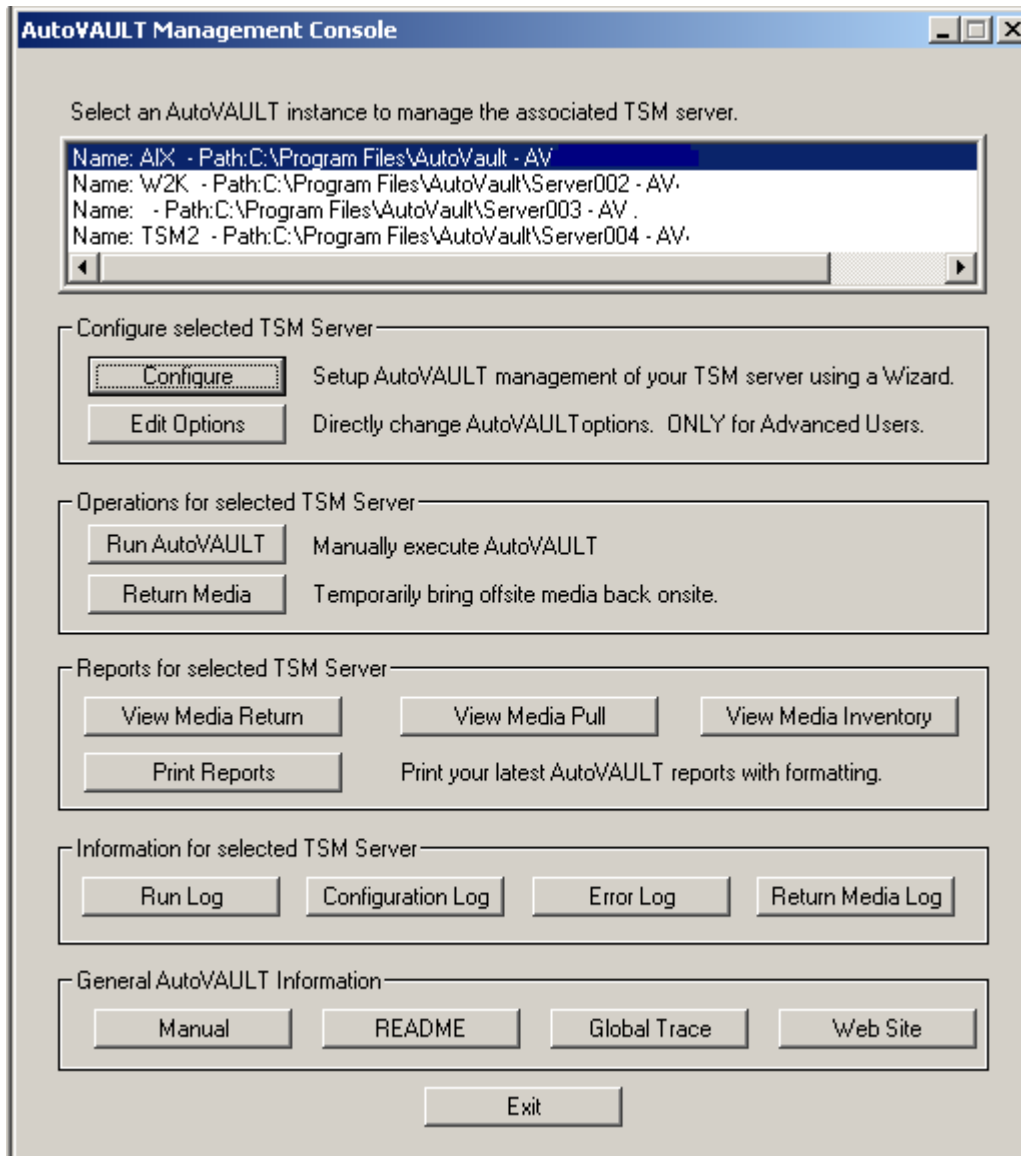
**Vault on Checkout Error** - Select whether AutoVAULT should record media as vaulted if the media checkout from the library fails. An error will be listed in the error log and on the tape pull report. If set to 'NO', AutoVAULT will not update the status of the media as offsite. If set to 'YES', AutoVAULT will update the status of the media as offsite.

**Reuse Delay** – Select a returning volume reuse delay. If greater than zero, returning volumes will be listed on the return report, but will not be made available to Storage Manager until the number of reuse delay days has expired. This option is useful when using private pooling. For example: You have a manual pool with a maxscratch of zero. When a vaulted tape becomes empty, AutoVAULT will list the tape on the return report and change the tape status to readwrite. Storage Manager could request the tape for a mount while it is still in transit back from the vault. By setting the Reuse Delay to '2', AutoVAULT will list the tape on the return report, but will not change the status to readwrite for two days allowing time for the tape to return onsite. In most cases, you would set this to the default value of “0”.

**Pre and Post Commands:** You can enter a command to be run before AutoVAULT runs, “pre”, or after AutoVAULT runs, “post”. The post command is often used to email the vault reports or ftp the recovery scripts offsite using the sample script avpost\_cmd.smp that was installed with AutoVAULT. Click “Create” to build file “avpost.cmd” from sample file “avpost\_cmd.smp”. Click “Edit” to edit either the pre-command or post-command file.

**TSM Post Command:** You can enter a TSM Administrative command to be executed after AutoVAULT runs. If you want to run multiple TSM commands, create a TSM Server Script and execute it from AutoVAULT.

## AutoVAULT Management Console



The AutoVAULT Management Console allows quick, centralized configuration, execution, and administration of your managed TSM instances. Highlight the TSM server instance you wish to work with and select an option below.

The “Name” is the name you assigned to this server instance when configured it using the AutoVAULT configuration wizard. You can use this name as parameter input to the `autovault.exe`. The “Path” is the location where all data for this TSM server instance is stored. Lastly, the AutoVAULT license key for this TSM server instance is displayed.

**Configure** - Select to run the AutoVAULT configuration wizard for the selected TSM instance.

**Edit Options** - Select to manually edit the AutoVAULT vault.opt option file. This should only be used by Advanced users.

**Run AutoVAULT** - Select to manually execute AutoVAULT for the selected TSM instance. The correct parameter option will be created for you

**Return Media** - Select to exclude media from normal operations for temporary use onsite for a recovery.

**View Media Return, Media Pull, or Media Inventory** - Select to view the latest AutoVAULT report for the selected TSM instance.

**Print Reports** - Select to print or reprint your latest TSM reports using AutoVAULT print formatting.

**Run Log** - Select to view the latest trace.txt file containing detailed execution output for the selected TSM server instance. This is a very useful log for problem determination.

**Configuration Log** - Select to view the latest tracecfg.txt file containing configuration output for the selected TSM server instance. This is very useful for problem determination of the configuration wizard.

**Error Log** - Select to view error messages from AutoVAULT execution of the selected TSM server instance.

**Return Media Log** - Select to view the latest tracertrn.txt file containing output from running 'Return Media' for the selected TSM server instance.

**Manual** - Select to open the AutoVAULT manual as a PDF.

**README** - Select to open the AutoVAULT readme.txt file

**Global Trace** - Select to view the avtrace.txt file containing detailed execution output that is not unique to a particular TSM server instance.

**Web Site** - Select to launch the AutoVAULT Home Page

# AutoVAULT Operations Guide

## Running or Scheduling AutoVAULT

Once AutoVAULT has been installed and configured, it should be scheduled to run using whatever mechanism you are comfortable with using. This might be Tony the operator, who is a whiz at using icons on the desktop to start programs in a timely fashion. Or, you might choose a method that is somewhat more automated.

AutoVAULT can be scheduled using any scheduling method with which you are comfortable. We recommend running AutoVAULT as a scheduled command from the Storage Manager Central Scheduler. By doing this, the operation of AutoVAULT is accessible through the same interface you already use to schedule your database and onsite storage pool backups.

When scheduling AutoVAULT to run with the Storage Manager scheduler from a path that contains a space, enclose the file and path in double quotes surrounded by single quotes. For example, to run from the default path, you would schedule a Storage Manager command action with either object:

```
"c:\program files\autovault\avr.run.bat" - NOTE: single quotes around double quotes (only valid in TSM V5)
"c:\progra~1\autovault\avr.run.bat" - NOTE: Only double quotes. This version will work with TSM Version 6
```

A command file is automatically created for each TSM server instance you add. The first TSM instance uses “avr.run.bat”. Additional instances use “avr.runxxx.bat” where xxx corresponds to the instance number and AutoVAULT path. For example, your second defined TSM server instance would use path c:\program files\autovault\SERVER002 and execution script:  
c:\program files\autovault\avr.run002.bat

One very efficient technique is to run all daily vaulting processes, including AutoVAULT, from a Storage Manager script. The example script below can be used to backup your primary pools to a copy pool, backup your Storage Manager database, and run AutoVAULT via the Storage Manager Central Scheduler. Note that the AutoVault server or workstation must be defined as a TSM client node with the Scheduler running in PROMPTED mode.

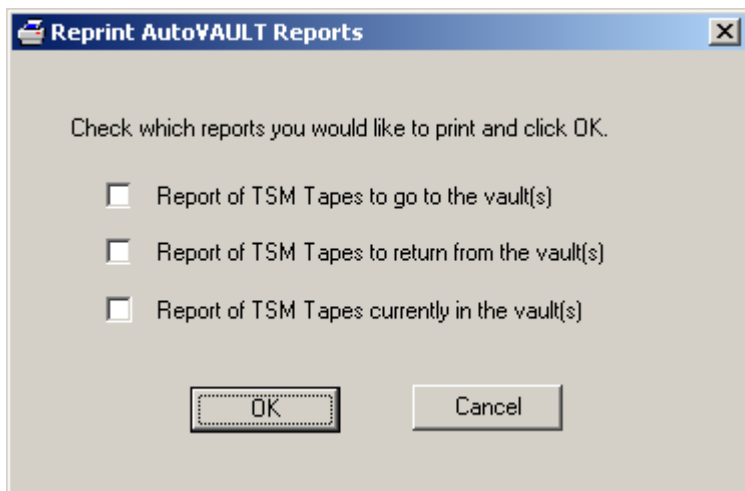
```
/* Process to create offsite backups */
/* */
/* Backup all primary storage pools */
ba stg backuppool cospool wait=yes
ba stg tapepool cospool wait=yes
/* */
/*backup the TSM database */
ba db t=f devclas=LTO wait=yes
/* */
/* Run AutoVault offsite Media Vaulting Process */
/* Run delayed to allow for tape dismount */
del sched standard autovault_run t=cl
def sched standard autovault_run t=cl act=command
    obj="c:\progra~1\autovault\avr.run.bat" startd=today
    startt=now+00:10 dura=15 duru=m peru=onetime day=any
def assoc standard autovault_run TSMSERVER
```

## Printing AutoVAULT reports

When you run the AutoVAULT configuration program, you can choose to print daily vaulting reports to the default printer. The Windows system account does not have a default printer. If you are running AutoVAULT via the Storage Manager scheduler and would like reports printed, you must run the Storage Manager scheduler from a userid with a default printer defined. You can set the default page orientation to Portrait or Landscape on the default printer to suit your needs. You can also change the default report font size using the AutoVAULT FONT parameter. Note that if you are also running backups from this service, the userid must have the proper authority for the server. A user with administrator authority is recommended.

When AutoVAULT runs, it creates three reports, which can be utilized in a number of ways. Each of these reports is a flat text file, which can be read using any available text editor, such as Wordpad. If you selected the 'print report' option during configuration, these reports will be printed to the default printer. You can also view the reports from the Storage Manager web administrative interface. Each report is stored separately in Storage Manager as a script. A nice option is to automatically email the reports to one or more people using an AutoVAULT post command.

If you need to reprint the most recent reports, use the "Print Reports" option from the AutoVAULT Management Console. The following screen displays allowing you to select which reports to reprint. You can select any defined printer as a destination. This will print the reports the same way that they appear from an AutoVAULT execution.



The most recent set of reports is written to the AutoVAULT install directory, usually

C:\Program Files\AutoVAULT\reports\ or C:\Program Files\AutoVAULT\SERVERxxx\reports\

Prior generations of the reports are kept in separate files with 001,002,...005 extensions. The three files are:

- `tapeoff.txt` report of tapes to be taken offsite to the vault
- `tapeon.txt` report of tapes to be returned from the vault

- `tapelist.txt` report of tapes that should be in the vault, including the tapes being sent to the vault from the current run of AutoVAULT

## Emailing AutoVAULT Reports

AutoVAULT installs a freeware mail client which you can use to email reports. It is easy to add this as a post command (see `POSTCMD` option) run when AutoVAULT execution completes. A sample command file is included in the AutoVAULT installation directory and at the root of every TSM server instance subdirectory. Rename "`avpost_cmd.smp`" to "`avpost.cmd`" and follow the instructions in the script.

## Protecting AutoVAULT

AutoVAULT stores some information in the Storage Manager database, but a large portion is stored in the AutoVAULT install directory. Regular backups of the AutoVAULT install directory are highly recommended, preferably at a time when AutoVAULT is not running.

## Moving AutoVAULT

AutoVAULT can be moved to a new location by following these steps:

- Backup the existing AutoVAULT installation directory
- Install the same version of AutoVAULT at the new location, but do not run configuration
- Copy the AutoVAULT install directory from the old location to the new location replacing duplicate files.
- Run AutoVAULT configuration for each TSM server instance and make any changes for the new location
- Review all PRE and POST command scripts and make changes for the new location.

## Creating Client Node Disaster Recovery Instructions

You may want to document specific recovery instructions for each node that Storage Manager backs up. This information can be entered as a Storage Manager script and will be saved in the Storage Manager database. It will therefore be backed up by a database backup and restored by the Disaster Recovery Scripts.

We recommend using a unique naming convention for the scripts such as '`DR_<nodename>`', where '`nodename`' is the Storage Manager nodename. You can also include a restore priority in the description line for future reference. For example, if you use the literal '`Priority x`' (where `x` is a number from one to five), you can identify the order in which server recovery should occur. You can easily generate a report of which servers are associated with each priority by running the following SQL query from an administrative command line:

```
Select NAME from SCRIPTS where COMMAND like '%Priority 1%' and NAME like 'DR_%' (Note that the 'like' search value is case sensitive)
```

This will return the name of all scripts that are restore priority one. Following is an example of a disaster recovery documentation script for a client node:

**Name:** DR\_FILESERVER01

**Description:** Disaster Recovery Instructions - Priority 1

**Lines:**

```
/* Instructions:
/*
/*     User specific recovery instructions
/*
/* Hardware and Software inventory:
/*
/*     Server specific information
/*
/* Contact Information
/*
/*     Technical Support
/*     Vendor contact information
```

## Returning Media from the Vault

**Return Offsite Volumes**

Retrieve Media

Database Backup Volumes

- M00158 2006-12-09 07:07:22.0000
- M00125 2006-12-10 07:11:13.0000
- M00145 2006-12-11 07:07:29.0000

Backup Set Volumes

Copy Pool Volumes

- M00089
- M00103
- M00119
- M00131
- M00135
- M00136
- M00153

Database Snap Backup Volumes

- M00084 2006-06-22 20:52:02.0000

Primary Pool Volumes

- M00104
- M00122

Retrieve Selected Volumes

Release Media

This media has been returned prematurely for use onsite. AutoVAULT will not process this media until you release it. Check the volumes that are no longer needed and click "Release Media" .

You must manually send the media back offsite if needed.

Release Media

- M00135
- M00136
- M00127
- M00084
- M000311
- M00091
- M00153

Exit

If you need to return vaulted media, use the "Return Media" option from the AutoVAULT Management Console. You can select one or more media volumes to return onsite. AutoVAULT will not process the selected media until you manually release the media from this screen. When you select "Retrieve Selected Volumes", you can print a Return report to give to your courier. A unique file, `tapeon_restore.txt`, is created in the `\reports` directory to interface the information to external software. If the AutoVAULT QwikScan™ interface is enabled, it will process this file.

If you would like to run this option remotely, please refer to the section "Remote Access to AutoVAULT".

## Remote Access to AutoVAULT

You may want to remotely access AutoVAULT to run it or return offsite volumes. You can use any remote access software such as pcAnywhere, Timbuktu, or VNC. On a Windows 2000 and 2003 Server, graphical remote access is included with the base product through Terminal Services. On a Windows XP Professional workstation, you can use Remote Desktop to remotely access AutoVAULT.

## QwikScan™ Interface

QwikScan is an open-system media manager product from NER data products inc. providing added functionality including tracking media movement by barcode ID and managing random slot vaulting. For more product information, visit [www.nerdata.com](http://www.nerdata.com)

Support has been added to automatically update QwikScan with media changes initiated by AutoVAULT. Whether you are running AutoVAULT manually, automatically, or manually returning media onsite using the AutoVAULT “Return Vaulted Volumes” feature, the data will be automatically communicated to QwikScan.

To enable the QwikScan Interface:

- Add or change the “qwikscan” option to “yes” in the AutoVAULT option file, “vault.opt”, located in the AutoVAULT installation directory
- Copy file “qwikscan\_copy\_bat.smp” in the AutoVAULT server instance directory to file “qwikscan\_copy.bat”
- Edit “qwikscan\_copy.bat” and change the paths of the AutoVAULT install directory, TSM instance directory, and the shared directory on the QwikScan server. Be sure that the userid running AutoVAULT has permission to write to the directory shared on the QwikScan server.
- Configure Qwikscan to read the AutoVAULT interface files. Each file is date and time stamped to allow for multiple executions.

## Checking in Media

Usually, you will want to check media into your tape library at a different time of day than when AutoVAULT runs. Instead of running CHECKIN manually, you can schedule it using a Storage Manager Script. The CHECKIN command cannot be directly scheduled using the TSM administrative scheduler. Create a Server Script named 'CHECKIN' with a line similar to "checkin libv QUALSTAR search=yes stat=sct" for each tape library. If you are running TSM v5.3 or later and want to eliminate the prompt for the checkin command, add “waitt=0” to your “checkin libv” command. Create an administrative command schedule to execute the Storage Manager Script (Command: run checkin). If your operators insert returning scratch tapes into the library during the day, schedule the checkin to run once a day in the evening.

## Gresham EDT-Distributape

AutoVAULT creates two files containing the volume names of media to move offsite and return onsite. The files tapeoff\_volumes.txt and tapeon\_volumes.txt are located in the autovault\reports or

autovault\SERVERxxx\reports directory. You can use the tapeoff\_volumes.txt file as input to the Distributape eject\_vol command to eject media from your tape library. For example: “eject\_vol -c <capID> -l tapeoff\_volumes.txt -d <ejectcount>”

## AutoVAULT Parameter Input

The autovault.exe executable will accept the following parameter:

SERVER=#x,@y,“Customer Name” or SERVER=ALL

### Where:

**x** is a numeric value corresponding to the path for the TSM server instance in AutoVAULT.

**y** is a numeric value for the number of minutes that AutoVAULT should sleep.

“**Customer Name**” is a user-defined name for the TSM server instance

“**ALL**” will run all defined TSM server instances in series

**Default:** For a single TSM server definition, the default is to execute AutoVAULT. When multiple TSM servers are defined, there is no default and a valid SERVER parameter MUST be entered.

**Example:** will run the TSM server defined in <avinstall directory>/SERVER002 then sleep 30 minutes, then run the same TSM server instance again.

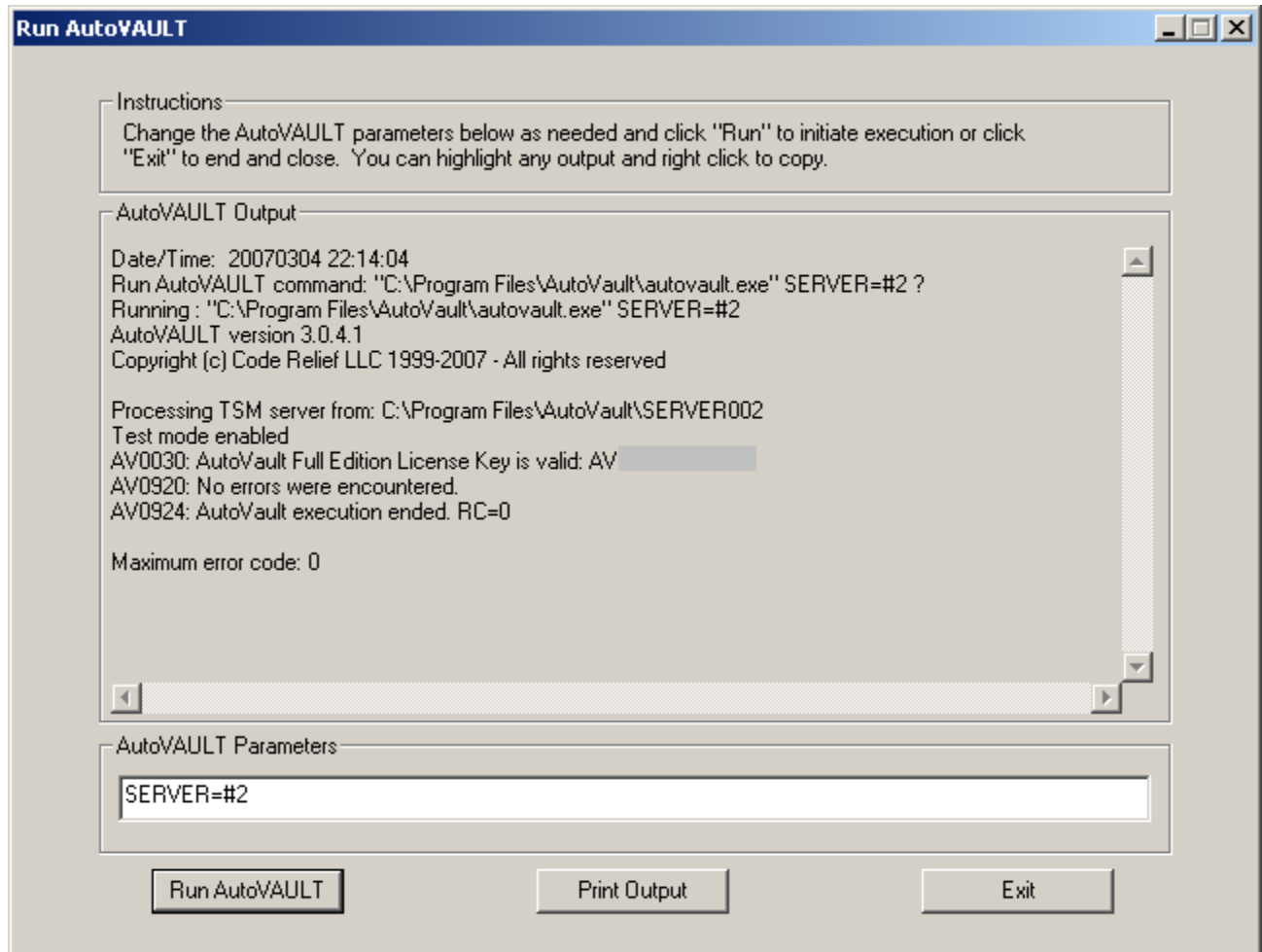
```
“autovault SERVER=#2,@30,#2”
```

**Example:** will run each of the three TSM servers in series using the customer-defined name for each instance.

```
“autovault SERVER=Reading, NewYork, Denver”
```

## Running AutoVAULT Manually

You can run AutoVAULT manually from the AutoVAULT Management Console by highlighting the TSM server instance and selecting “Run AutoVAULT”. The following screen will display with the correct AutoVAULT SERVER parameter already inserted. You can change the SERVER parameter before execution. All output is kept in a scrolling window. You can print the output by selecting “Print output”. You can also highlight any output and copy it.



## Suppressing TSM Informational Messages

There is a way to disable messages that are generated when AutoVAULT runs. You can disable them for CONSOLES, the ACTLOG, or both. The following three TSM commands will disable the session established, session ended, and command issued messages for only your TSM consoles.

```
DISABLE EV CONSOLE ANR0405
DISABLE EV CONSOLE ANR0407
DISABLE EV CONSOLE ANR2017
```

This will remove a lot of the messages from your operators consoles making them more usable. You can also remove them from the activity log using 'DISABLE EV ACTLOG msgid'

## Audit Log - Tracking tape usage

AutoVAULT maintains an audit log file, `av_audit_log.csv`, in the debug directory of the corresponding server instance. The log data is in CSV format and can be viewed with Excel or another reporting tool. The columns of data in order are: Date, Time, Volume Name, Media Type, AutoVAULT Action, Pool Name, Vault Location, Tape Library Name, and Tape Library slot. A blank is inserted when there is no relevant data for a field. An entry is created every time AutoVAULT updates a tape. This is a useful tool for debugging a problem or tracking your media movements.

## Interface Files created by AutoVAULT

AutoVAULT creates several interface files that you can use for additional functions and scripting. The QwikScan™ interface uses these files to coordinate media changes to its external media management software, but you can also use the files for other uses. The following files are located in the AutoVAULT “reports” directory and are created every time AutoVAULT is executed. For all file names: “tapeon” indicates media moving onsite, “tapeoff” indicates media moving offsite, and “tapelist” indicates an inventory of all media currently offsite.

**tapeon\_volumes.txt, tapeoff\_volumes.txt** - These two files contain only the volume name of media that was moved onsite or offsite. They can be used to interface with Gresham EDT or other external media managers. The vault location is not included in these files

**tapeon\_volvault.txt, tapeoff\_volvault.txt, tapelist\_volvault.txt** - These three comma delimited files contain the volume name of media and the vault location name. They can be used to interface with QwikScan™ or other media management software.

**tapeon\_volumes\_<vault name>.txt, tapeoff\_volumes\_<vault name>.txt** - These files contain the volume name of media without the vault location name. **tapeon\_volvault\_<vault name>.txt, tapeoff\_volvault\_<vault name>.txt** - These comma delimited files contain the volume name of media and the vault location name. They contain the same data as the above files but have been separated into individual files with the vault location appended to the name. They can be used to interface with QwikScan™ or other media management software and are very useful when different software or vendors manage different vault locations.

## Automatically reporting to a Vaulting Company Like Vital Records Inc® or Iron Mountain®

At most vaulting companies, TSM media is considered "Open Media" (because each tape is tracked individually and expires at a different time) and not "Container Media" (which all comes back from the vault at once). Because of this difference, you need to tell your vaulting company which tapes to pick up and which ones to bring back.

If your vaulting company supports electronic reporting, AutoVAULT now allows you to automatically FTP your tape movement information in a method that they can easily process ... without daily intervention on your part! AutoVAULT creates interface files each time it runs: "TapeOn" for media moving onsite and "TapeOff" for media moving offsite. Without AutoVAULT, you must send daily forms to accomplish this task or write scripts to automate the process, which are often difficult to maintain. If you forget or send the wrong tape movement information, your important data backups may not be in the right place at the right time.

AutoVAULT creates several interface files that you can use for reporting media movements to your vaulting company. The sample AutoVAULT POST script, `avpost_cmd.smp`, contains a section for automatically reporting your tape movements to your vaulting company. This includes the list of media to request for onsite return. It also includes the list of media you are sending to the vaulting company so they can verify receipt. The script sample has details on setting up the process. You will need to edit `ftpvault.txt` with the ftp login credentials for your vaulting company. You will need to customize the script with your vaulting companies ftp site address. If you are using multiple vault locations, you will also need to edit which vault location is sent to the vaulting company.

This option will eliminate the need to use the vaulting companies web interface to request individual media for onsite return or pickup. You may also get the added feature of having the vaulting company report to you concerning media it did not receive, but was expecting. (If you use Vital Records Inc® or Iron Mountain®, everything has been fully tested. If you are using a different vaulting company that supports electronic reporting, you will need to contact your vaulting company and AutoVAULT support for some assistance in the initial setup.)

## Vault Location Changes

AutoVAULT does not store the vault location locally with each individual media. The vault location is assigned when AutoVAULT executes based on the value assigned to the media type. If you change the name of a VAULT location, AutoVAULT will report the changed name on all previously vaulted media as well as newly vaulted media. Note that the TSM "LOCATION" attribute associated with each individual media will not be updated for previously vaulted media. You can update this value in TSM if you wish. For example, you can use the TSM "UPD VOL \* LOC=<new location> WHERESTG=<poolname>" command to update the LOCATION of all media in a particular pool.

# Disaster Recovery

## ***Vaulting the Disaster Recovery Scripts***

The Disaster Recovery Scripts are created every time you run AutoVAULT. AutoVAULT recovery scripts are created in the AutoVAULT TSM instance directory in /avrecover/latest/\*.\*. If you are using DRM, IBM prepare recovery scripts are created in the AutoVAULT TSM instance directory in /ibmrecover/latest/\*.\*. We encourage you to take all the files in this directory offsite daily with your Storage Manager database backup and other media. One option is to copy the Disaster Recovery Scripts to a floppy, CD, or DVD. A sample script, "copyscript\_bat.smp" is included in the AutoVAULT installation directory. Rename the script to "copyscript.bat" and review the instructions in the script. A much better option is to ftp the Disaster Recovery Scripts to a remote location. A sample script, "avpost\_cmd.smp", is included in the AutoVAULT installation directory. Rename the script to "avpost.cmd" and follow the instructions in the script.

## ***IBM Prepare Recovery Scripts***

If you are using DRM, IBM prepare recovery scripts are created in the AutoVAULT TSM instance directory in /ibmrecover/latest/\*.\*. A new prepare is created for both a DBB and DBS recovery. The prepare files are then moved from the TSM server and renamed to "prepare\_dbb.txt" and "prepare\_dbs.txt". By using a static name for these files, you can easily FTP them offsite with the AutoVAULT post command file avpost.cmd or some other technique.

## ***AutoVAULT Recovery Scripts***

### Customizing the Disaster Recovery Scripts

You may want to include information specific to your installation with the recovery scripts such as employee contact information. All information included in the file:

<AV\_TSM\_instance>\avrecover\INSTRUCTIONS\_CUSTOM.TXT

will be included with the recovery scripts. Edit this file with any instructions you wish to include.

### Disaster Recovery Script Details

Each time AutoVAULT runs, it creates an updated set of scripts that can be used to restore your Storage Manger Server. The scripts are to be run natively on your Storage Manager Server after you have installed the operating system and Storage Manager. The scripts will:

- Restore your device configuration, volume history, and server option files.
- Reallocate and format your database and log volumes.
- Restore your database from the latest backup.
- Register your Storage Manager Licenses.
- Update all onsite volumes as destroyed and all offsite volumes as available.

The latest recovery scripts are located in the AutoVAULT install directory: <AV TSM instance>\avrecover\latest\. All files in this directory should be vaulted on removable media, such as a floppy, CD, or DVD or ftped offsite each time you run AutoVAULT. See the section “Vaulting the Disaster Recovery Scripts” above for instructions.

The following files are included with the recovery scripts:

cdestroy.txt	Copy Pool volumes that were onsite and destroyed.
creadw.txt	Copy Pool volumes that were offsite and available to restore from.
dbvol.txt	List of full path database volumes.
devconfig	Device Configuration File
dsmserv.opt	Storage Manager option file
lic_reg.txt	Storage Manager license registration information.
logvol.txt	List of full path log volumes.
pdestroy.txt	Primary Pool volumes that were onsite and destroyed.
preadw.txt	Primary Pool volumes that were offsite and available to restore from.
readcust.txt	Customer specific restore instructions and information copied from <AV_install>\avrecover\INSTRUCTIONS_CUSTOM.TXT.
readme.txt	Detailed Disaster Recovery Instructions.
restore1.cmd	Phase one of the Storage Manager Server restore.
restore2.cmd	Phase two of the Storage Manager Server restore.
restore3.cmd	Recreate your Primary Pool storage volumes
servrcfg.txt	Detailed information about your Storage Manger Server environment.
tapelist.txt	The latest vaulted tape inventory listing .
volhist	Volume History File

## Disaster Recovery Instructions Example

Included with the Disaster Recovery Scripts are instructions to restore your Storage Manager Server, located in file README.TXT. Following is an example of the recovery instructions that AutoVAULT creates.

\*\*\*\*\*

Generated by AutoVault on 20070204 07:13:15

AutoVault Windows Server recovery instructions

\*\*\*\*\*

The following steps will restore your TSM server environment to its state as of your last available backup. This assumes that all database backups and copypool tapes are available for use.

Review file READCUST.TXT for additional information for your site.

1) Install Windows Server and all service packs on the recovery server. Your original Windows server version was:

Windows version 5.0 Service Pack 4

2) Install TSM server software. Your TSM sever was at version:

Storage Management Server for Windows - Version 5, Release 4, Level 0.0

TSM Server instance install path: C:\Program Files\Tivoli\TSM\server  
TSM install path: C:\Program Files\Tivoli\TSM\Server

Run the TSM Configuration wizard to recreate your TSM server instance. If you are running multiple TSM server instances, use the wizard to recreate them all.

3) Create directory c:\avrecover on your TSM server and copy the latest recovery script files into the directory. The latest recovery script files are the ones you saved from your original TSM server located in the autovault install directory in <AutoVault install directory>\avrecover\latest\\*.\*

4) Review file c:\avrecover\tapelist.txt and verify that all volumes listed are currently available. Retrieve them from the vault.

5) Define your tape hardware. If your server configuration is exactly the same as your original TSM server, skip this step.

TSM Manuals are available online at:

<http://publib.boulder.ibm.com/infocenter/tivihelp/index.jsp>

In most situations, your recovery server is configured differently than your original server. The AutoVault recovery scripts need information about the tape hardware on the recovery server in order to run successfully. This information is saved in the device configuration file: c:\avrecover\devconfg. You will need to edit this file to match the hardware on the recovery server.

The quickest way to create a new device configuration file is to use the TSM Server Utilities. The TSM Device Configuration Wizard will step you through defining your new tape hardware. Since this was a new install of TSM, you will need to use the default administrator signon, userid: admin password: admin.

After you have created new devices, save the device configuration file by issuing command 'BA DEVCONFIG' from an TSM administrative command line. If you did not specify a device configuration file, add 'DEVCONFIG devconfig.out' to your TSM server option file, dsmserv.opt, and restart the TSM server. Copy the tape drive and library device configuration information from the device configuration file usually in the TSM server directory and replace the tape drive and library device configuration information in file to c:\avrecover\devconfg.

#### Example:

```
/* Device Configuration */  
DEFINE DEVCLASS 8MMCLASS1 DEVTYPE=8MM FORMAT=DRIVE MOUNTLIMIT=DRIVES MOUNTWAIT=60  
MOUNTRETENTION=1 PREFIX=ADSM LIBRARY=LB3.0.0.0  
SET SERVERNAME HSERVER2  
DEFINE LIBRARY LB3.0.0.0 LIBTYPE=SCSI DEVICE=LB3.0.0.0 SHARED=NO  
DEFINE DRIVE LB3.0.0.0 MT4.0.0.0 DEVICE=MT4.0.0.0 ELEMENT=82 ONLINE=Yes  
DEFINE DRIVE LB3.0.0.0 MT6.0.0.0 DEVICE=MT6.0.0.0 ELEMENT=83 ONLINE=Yes
```

6) Update your tape library volume location information. If you are using a manual library to recover, skip this step. Place the physical database backup volumes in the automated tape library and note the home element location of each volume. Edit c:\avrecover\devconfig and update the volume names and home element location for each volume. Delete the volume location for any volume that is not in the library.

Example:

```
/* LIBRARYINVENTORY SCSI LB3.0.0.0 CR0001 1 101*/  
/* LIBRARYINVENTORY SCSI LB3.0.0.0 CR0002 2 101*/  
/* LIBRARYINVENTORY SCSI LB3.0.0.0 CR0005 5 101*/  
NOTE: the fifth value is the home element
```

7) Verify that you have the correct disk volumes with enough space on them to restore your TSM database and log files. Open file c:\avrecover\servrcfg.txt. Search for "dbvol". Note the location and size of each database volume. Search for "logvol". Note the location and size of each log volume. If the drives or required space are not available, edit files c:\avrecover\logvol.txt and c:\avrecover\dbvol.txt and change the location to match your new server. Note that the space must be equal or greater to that originally required. All values are in MB.

8) Consider adding server option "DISABLEScheds Yes" to your TSM server options file located at c:\avrecover\dmserv.opt. This option will disable all administrative and client schedules which may interfere with your restore process. You can remove this option later after all data has been restored to return your server to its original operating schedule.

9) Edit c:\avrecover\restore1.cmd. Verify that the TSM server path variable 'server\_path' is correct. The path should not contain spaces. Use the 8.3 format of the directory if it contains a space. For example, "C:\Program Files\Tivoli\TSM\server\" would be "C:\PROGRA-1\Tivoli\TSM\server\". Make sure that the TSM server is not running.

From a command prompt, run:

```
c:  
cd c:\avrecover  
restore1.cmd
```

This script will:

- Create and format your database and log files
- Restore your database from your latest offsite tape(s)
- Start the TSM server in the foreground.

10) Edit c:\avrecover\pdestroy.txt and remove any volume that is currently available.

11) Edit c:\avrecover\cdestroy.txt and remove any volume that is currently available.

12) Edit c:\avrecover\creadw.txt and remove any volume that is not currently available.

13) Edit c:\avrecover\preadw.txt and remove any volume that is not currently available.

14) Edit c:\avrecover\restore2.cmd. Verify that the TSM client path variable 'client\_path' is correct. Verify that a valid administrator userid and password are set for variables 'admin' and 'password'.

From a command prompt, run:

```
c:
cd c:\avrecover
restore2.cmd
```

This script will:

- Register your TSM licenses. License information is not stored in the database.
- Mark all offsite media as available
- Mark all onsite media as destroyed

15) If your tape hardware has changed in any way from your original configuration, you will need to define the new libraries and drives to the TSM server. Your old definitions exist at this point, but they probably do not match your current hardware configuration. The quickest way to create new device configurations is to use the TSM Server Utilities. The TSM Device Configuration Wizard will step you through defining your new tape hardware. NOTE: if you already did this before restoring your database, you still need to do it again.

Those definitions were overwritten by the database restore. You may be able to just update the DEVICE for your library(s) and drive(s) to match the new device name if your tape hardware is identical, but the device is incorrect. If the tape hardware is completely different, define the new LIBRARY(s) and DRIVE(s) and update your DEVCLASS to reflect the new library name.

16) You are now ready to run restores of client data.

17) After you have restored your client data, you may need to run backups. This will require you to define replacement primary pool volumes. DO NOT DELETE ANY EXISTING PRIMARY POOL VOLUMES. If you delete an existing primary pool volume, you will not be able to restore any of that data from the cypool. AutoVault creates two TSM server scripts which will define replacement primary pool volumes and restore all the data from cypool(s). To create the server scripts, run the following command from an administrative command line client on your TSM server: 'macro c:\avrecover\restore3.cmd'. This TSM macro will create server script 'av\_restore\_ppool\_vols' which you can edit and run to define replacement disk and sequential primary pool volumes. It will also create server script 'av\_restore\_ppools' which you can edit and run to restore data to your primary pools from the copy pool(s). The TSM server scripts are easiest to review and edit through the TSM administrative web interface. You can run the server script from the web interface. You can also run the server scripts from the command line interface using 'RUN <script name>'. Note that AutoVault appends '@' to all volume names so they are unique.

# Reference

## **AutoVAULT Options Reference: the vault.opt file**

AutoVAULT uses an option file that is very similar to those used by Storage Manager to determine its behavior.

### **Audit Log Retention option: the AUDITLOG option**

The AUDITLOG option controls how many days of tape activity to retain in the log. The audit log file, av\_audit\_log.csv, can be found in the debug directory of the corresponding server instance.

Example: AUDITLOG 365

**AUDITLOG** <Number of Days>                      DEFAULT - 365

### **Backup Sets vault option: the BKSVAULT option**

The BKSVAULT option controls whether client backup sets are included for vaulting and which vault name is assigned. If this option is YES, all backup sets will be sent offsite and retained there until they expire. Example: BKSVAULT YES,OFFSITE

**BKSVAULT** [YES|NO],<Vault Name>                      DEFAULT - NO

### **Specifying copypools to manage: the COPYPOOL option**

Copy storage pools are probably where the bulk of AutoVAULT's work will be done. The COPYPOOL option allows you to specify which copy storage pools you want to manage using AutoVAULT and which vault name is assigned. You can limit vaulting to only FULL media or process ALL media. Specifying copypools can be accomplished either with a wildcard or by specifying each copypool that you want to manage with a separate COPYPOOL statement. If you use the \* wildcard (this is the default), all Storage Manager copy storage pools will be managed by AutoVAULT. If there are copypools that you do not want to be managed by AutoVAULT, such as onsite copypools, you must explicitly select each copypool that you want vaulted. Example: COPYPOOL \*,OFFSITE,ALL

**COPYPOOL** [<CopyPool Name>|\*],<Vault Name>,[ALL,FULL]    DEFAULT – All Copypools

### **Database backup vault option: the DBBVAULT option**

The DBBVAULT option controls whether Storage Manager full and incremental database backups are included for vaulting and which vault name is assigned. If this option is YES, all full and incremental database backups will be sent offsite and retained there until they expire. Example: DBBVAULT YES,OFFSITE

**DBBVAULT** [YES|NO],<Vault Name>                      DEFAULT - YES

## Database backup cycles to retain: the DBCYCLE option

The DBCYCLE option controls the number of Storage Manger database backup cycles to retain.

If DRM processing is selected, this will set the value of DRMDBBACKUPEXPIREDDAYS. The larger of the DBCYCLE or DBSCYCLE values will be used to set DRMDBBACKUPEXPIREDDAYS. Selecting a value of zero will disable the setting of this TSM parameter.

If not using DRM processing, a value greater than zero enables the deletion of full and incremental database backup series (where a series is a full backup and all subsequent incremental backups). AutoVAULT will delete all older backup series and retain only the number of series you specify. Selecting a value of zero will disable the deletion of full and incremental database backups.

We recommend that you configure your copy pools with the REUSEDELAY parameter set to a number of days that will allow all volumes referred to by the oldest series of database backups to stay in the vault during the course of normal operations. For example, if you configure AutoVAULT with DBCYCLE set to five, you might want to configure the copy pools with the REUSEDELAY parameter set to eight. This would take into account the lag caused by a long weekend where processing did not occur. This strategy will increase the number of tapes required for your backup/recovery operations, but not adopting this approach increases the probability of unrecoverable data loss should you need to revert to an older database backup. Example: DBCYCLE 5

**DBCYCLE <number of cycles to retain>**                      DEFAULT - 5

## Database snapshot backup cycles to retain: the DBSCYCLE option

If DRM processing is selected, this will set the value of DRMDBBACKUPEXPIREDDAYS. The larger of the DBCYCLE or DBSCYCLE values will be used to set DRMDBBACKUPEXPIREDDAYS. Selecting a value of zero will disable the setting of this TSM parameter.

If DRM processing is not selected, the DBSCYCLE option controls the number of database snapshot backup cycles to retain. A value greater than zero enables the deletion of snapshot database backups. AutoVAULT will delete all older backups and retain only the number of backups you specify. AutoVAULT will never delete the last remaining database backup. Selecting a value of zero will disable the deletion of snapshot database backups. Example: DBSCYCLE 5

**DBSCYCLE <number of cycles to retain>**                      DEFAULT - 5

## Database snapshot backup vault option: the DBSVAULT option

The DBSVAULT option controls whether Storage Manager snapshot database backups are included for vaulting and which vault name is assigned. If this option is YES, all snapshot database backups will be sent offsite and retained there until they expire. Example: DBSVAULT NO,OFFSITE

**DBSVAULT [YES|NO],<Vault Name>**                      DEFAULT - NO

### **Use DRM for media processing option: the DRMUSE option**

The DRMUSE option enables the use of MOVE DRMEDIA and MOVE MEDIA commands for media movement. Backupsets are not supported by MOVE commands and will be processed with the CHECKOUT command. Example: DRMUSE YES

**DRMUSE [YES|NO]                      DEFAULT - YES**

### **Purging entries in the AutoVAULT log: the ERRLOG option**

AutoVAULT updates a log file, **errorpt.txt**, every time it runs. This log can be reviewed for normal completion and errors. Entries are stamped with a date and time. The ERRLOG option specifies the number of days of log information to retain. AutoVAULT will delete entries in the log that are older than the specified number of days. Example: ERRLOG 30

**ERRLOG <number of days to retain>                      DEFAULT - 30**

### **Report font size: the FONT option**

AutoVAULT allows you to change the report font size by setting the FONT parameter in vault.opt. This parameter is not available for edit during AutoVAULT configuration and must be manually edited. You can also change the page orientation of your default printer whether you are running AutoVAULT manually or automatically. By increasing the font size and changing the page orientation to Landscape, you can enlarge the reports for easier reading. The default font is “Courier New” and cannot be changed. Example: FONT 10

**FONT <size>                      DEFAULT - 8**

### **Report FTP errors: the FTPERROR option**

Set to 'YES' if AutoVAULT should generate an error if an ftp process fails. Ftp is used to transfer files from a remote TSM server for recovery. This parameter should only be set to NO if you have another way to recover the TSM server and do not want ftp failures of key recovery files reported as errors. Example: FTPERROR Yes

**FTPERROR [YES|NO]                      DEFAULT - YES**

### **Using passive FTP: the FTPPASSIVE option**

Set to 'YES' to use passive ftp to transfer files from a remote server. Example: FTPPASSIVE NO

**FTPPASSIVE [YES|NO]                      DEFAULT - NO**

### **Selecting the Windows Server Instance: the ISERVER option**

If more than one Storage Manager instance is defined on a Windows server, use the ISERVER option to select which instance AutoVAULT should manage. Example: ISERVER 2

**ISERVER <TSM Server Instance>                      DEFAULT - 1**

## Defining libraries to AutoVAULT: the LIBRARY option

The LIBRARY option allows you to configure AutoVAULT to interact with different libraries attached to your server. The parameters of the LIBRARY option control the manner in which AutoVAULT checks tapes out of the library.

**LIBRARY=<libname> REM=[yes|no|bulk],CHECKL=[yes|no],MAXCHECKOUT=<number>**

The name of the library is specified first. The other parameters can be specified in any order. The functions of the LIBRARY option parameters correspond exactly to the parameters of the CHECKOut command. The following paragraphs describe the parameters and their implications here.

The REM parameter controls whether AutoVAULT will have Storage Manager physically eject the tape from the library. Typically this is turned on only when you have some mechanism built into the library for inserting and removing tapes, sometimes referred to as an I/O port.

REM=yes will display a message on the server console prompting the operator for a reply to the message to remove the tape. In most circumstances, this is not an effective way to check tapes out of the library. According to the Storage Manager documentation, this parameter will eject a volume from an IBM 3494 or 3495 library into the bulk I/O station.

REM=no leaves the volume in the library, but deletes it from the Storage Manager library inventory. This is the quickest method to check volumes out of a library. You then need to manually remove the volumes after AutoVAULT has reported the names of the volumes that are to be sent to the vault.

REM=bulk will cause the volume to be ejected to the next available Entry/Exit port (or I/O port). No prompting occurs, and no REPLY is required as with REM=yes.

The CHECKL parameter controls whether you want Storage Manager to check the label of the tape before checking it out of the library.

CHECKL=No assumes that you trust Storage Manager's records of where a particular tape volume is kept and do not want to take the time to verify that the physical tape in a particular slot is the same as the tape that Storage Manager believes to be there. Normally, this is a pretty safe assumption, but circumstances can arise where this is not the case. (Typically, this requires an audit of the library by Storage Manager to correct the problem.)

CHECKL=Yes will cause AutoVAULT to request that the tape label be read before checking the tape out of the library. The tape will be mounted in a drive and the tape header read to verify that it corresponds to what Storage Manager thinks should be in that particular tape slot. (You are probably well aware of this fact, but this can be quite time-consuming, especially if you have several tapes to check out.)

MAXCHECKOUT={number} specifies that a volume is ejected to the next available I/O port until the value of MAXCHECKOUT is reached. This option is only used if you specify REM=BULK. AutoVAULT assumes the number of I/O ports you select is available and will continue to eject media until those slots are full. If more media must be ejected than the selected number of I/O ports, then AutoVAULT will issue an error and will not vault the

media. You should empty the I/O ports and run AutoVAULT again to checkout the remaining media.

Setting the MAXCHECKOUT value to '0' disables this option. If set to '0', AutoVAULT will fill all the I/O ports. If more media must be ejected than the number of physical I/O ports, then you must manually eject the media from the tape library.

DEFAULT – REM=no, CHECKL=no for all libraries

Example: LIBRARY REM=BULK,CHECKL=NO,MAXCHECKOUT=5

### **Running AutoVAULT in test mode: the MODE option**

Changing the MODE option to DEBUGTEST will disable the update of TSM information, but will allow AutoVAULT to simulate execution. This is useful to try AutoVAULT without changing the status of your TSM server. Example: MODE DEBUG

**MODE [DEBUG, DEBUGTEST]            DEFAULT - DEBUG**

### **Check for vaulted media onsite: the ONSITECHK option**

AutoVAULT looks in your defined tape libraries for media that has already been sent offsite. AutoVAULT will send it offsite again if found. Setting this option to NO will disable the scan of tape libraries for previously vaulted media. Example: ONSITECHK YES

**ONSITECHK [YES|NO]            DEFAULT - YES**

### **Specifying a command to run after AutoVAULT executes: the POSTCMD option**

Use this option to execute any operating system command after AutoVAULT executes. One use of this option is to email the AutoVAULT reports to one or more people. You could also use this option to send the reports to one or more non-default printers. (For example, the default printer for the userid that the Central Scheduler service is running under may not be anywhere near where the operations staff or the tape library are located.)

The POSTCMD option can be specified only once. If you need to perform multiple actions after AutoVAULT runs, you must combine them using a script (e.g. Batch or Perl) or an executable.

GBMail, an SMTP email utility, is installed with AutoVAULT and can be used to send email using any SMTP mail server. A batch file, **email\_bat.smp**, is also installed and can be edited for your location. For details of the operation of GBMail, refer to the [Using the GBMail client](#).

**POSTCMD <command to execute>            DEFAULT - None**

Example: POSTCMD "C:\Progra~1\AutoVAULT\avpost.cmd"

### **Specifying a command to run before AutoVAULT executes: the PRECMD option**

Use this option to execute any operating system command before AutoVAULT executes.

**PRECMD** <command to execute>                      DEFAULT - None

### **Specifying primary and active data storage pools to move offsite: the PRIMARYPOOL option**

Offsite relocation of primary and active data storage pool volumes is a feature of AutoVAULT that allows you to make better use of your library capacity. Storage Manager considers all primary storage pools to be local and readily available, which for many circumstances makes perfect sense. But what if the data stored in one or more of your primary pools is very static, referenced infrequently, and has long retention periods? Use this option to vault a primary pool to an onsite or offsite vault. You can limit vaulting to only FULL media or process ALL media. You can also limit vaulting to media that has not been referenced in x number of days. If you limit vaulting to only FULL media unreferenced in x days, then both criteria must be met before the media will be processed.

Example: PRIMARYPOOL ARCHIVE,ONSITE,FULL,0

**PRIMARYPOOL** <pool name>,<vault name>,[ALL,FULL],<days since use>

DEFAULT – No primary pools are managed

### **Specifying report printing: the PRINTRPT option**

Use this option to select whether AutoVAULT reports should be printed to the default printer. AutoVAULT creates reports of volumes to move offsite to the vault, volumes to return onsite from the vault, and all volumes currently in the vault. You can select which reports are printed using the RPTSELECT option. If you choose to also store reports as a Storage Manager script, they will be available through an administrative web or command line interface.

If you are running AutoVAULT automatically using the Storage Manager Scheduler Service, you will need to run the service under a user with a default printer assigned. The Windows system account does not have a default printer. If you would like reports printed, you must run the Storage Manager scheduler from a userid with a default printer defined. Example: PRINTRPT YES

**PRINTRPT** [YES,NO]                      DEFAULT - No

### **Enabling the QwikScan™ Interface: the QWIKSCAN option**

Use this option to enable the QwikScan™ Interface. QwikScan can track media movement using the barcode id and allow for random slot filling. AutoVAULT can automatically pass tape movement information to QwikScan or other external management software so its inventory is kept current. Refer to the section in this manual on the QwikScan Interface for more details. Example: QWIKSCAN YES

**QWIKSCAN [YES,NO]**                      DEFAULT - No

### **Specifying when to make returning tapes available: the REUSEDELAY option**

Use this option to select a returning volume reuse delay (specified in days). This option is not valid with DRM. If greater than zero, returning storage pool volumes will be listed on the return report, but will not be made available to Storage Manager until the number of reuse delay days has expired. For example: You have a manual pool with a maxscratch of zero. When a vaulted tape becomes empty, AutoVAULT will list the tape on the return report and change the tape status to readwrite. Storage Manager could request the tape for a mount while it is still in transit back from the vault. By setting the Reuse Delay to '2', AutoVAULT will list the tape on the return report, but will not change the status to readwrite for two days allowing time for the tape to return onsite. Example: REUSEDELAY 2

**REUSEDELAY <number>**                      DEFAULT - 0

### **Pull report heading: the RHPULL option**

Use this option to override the default heading on the tape pull report. A maximum of 70 characters can be used. Example: RHPULL Tapes Going Offsite

**RHPULL <report title>**                      DEFAULT - TSM Tapes to take Offsite to the Vault

### **Return report heading: the RHRETURN option**

Use this option to override the default heading on the tape return report. A maximum of 70 characters can be used. Example: RHRETURN Tapes Returning Onsite

**RHRETURN <report title>**                      DEFAULT - TSM Tapes to return Onsite from the Vault

### **Vault report heading: the RHVAULT option**

Use this option to override the default heading on vaulted tape report. A maximum of 70 characters can be used. Example: RHVAULT Tapes in the Vault

**RHVAULT <report title>**                      DEFAULT - TSM Tapes Currently in the Vault

### **Company report headings: the RPTHEAD option**

Use this option to include a unique heading, such as your company name, on all printed reports. A maximum of 70 characters can be used. Example: RPTHEAD Code Relief LLC

**RPTHEAD <report title>**                      DEFAULT - None

### **Sorting the Reports: the RPTORDER option**

Use this option to sort the new reports. If no RPTORDER option exists, the legacy report format will be used. Different sort criteria exist for each of the three reports. The criteria can be in any order. The report will be sorted using the criteria in order from left to right.

**RPTORDER      PULL,VAULT,LIBRARY,VOLSER,TYPE**  
**RPTORDER      RETURN,VAULT,VOLSER,TYPE**  
**RPTORDER      VAULT,VAULT,TYPE,POOL,VOLSER**

### **Selecting which reports to print: the RPTSELECT option**

Use this option to select which reports to print. The options are "PULL" for the report of tapes to go offsite, "RETURN" for the report of tapes to return onsite, "VAULT" for the report of all tapes in the vault, or "ALL" to print all reports. The options can be entered in any order separated by commas. The RPTSELECT option is only valid if the PRINTRPT option is "YES".

Example: RPTSELECT PULL,RETURN

**RPTSELECT [PULL,RETURN,VAULT | ALL]**                      DEFAULT – ALL

### **Specifying level of security: the SECURITY option**

Use this option to select the level of security for AutoVAULT processing. If low security is selected, the administrator and userid will be included in the disaster recovery scripts. If high security is selected, you will need to provide a valid administrator and password at disaster recovery time. Example: SECURITY LOW

**SECURITY [HIGH | LOW]**                      DEFAULT - High

### **Specifying TSM server FTP path: the SVFTPPATH option**

Use this option to tell AutoVAULT what FTP path to use on a remote TSM for Windows server. This will be a virtual path you define on the TSM server. It must contain the dsmserv.opt file for the server as well as a copy of the volume history and device configuration. Example: SVFTPPATH tsm\

**SVFTPPATH <virtual ftp path>**                      DEFAULT - <blank>

### **Specifying TSM server Hostname or IP address: the SVIP option**

Use this option to tell AutoVAULT the hostname or IP address of the TSM server. Example: SVIP tsmserver

**SVIP** [<hostname>|<ip address>]                      DEFAULT - <blank>

### **Specifying TSM server Install path: the SVPATH option**

Use this option to tell AutoVAULT the location that you installed the TSM server (DSMSERV\_DIR). For remote servers, this value is manually entered during configuration. For a local server, AutoVAULT sets this value from the registry during configuration. Example: SVPATH C:\Program Files\Tivoli\TSM\Server

**SVPATH** <TSM server install path>                      DEFAULT - <blank>

### **Specifying TSM server DSMSERV\_CONFIG path: the SVCPATH option**

Use this option to tell AutoVAULT the location of your TSM server configuration file since it can be in a different location than where you installed TSM (DSMSERV\_CONFIG). For remote servers, this value is manually entered during configuration and verified using FTP. For a local server, AutoVAULT sets this value from the registry during configuration. Example: SVCPATH C:\Program Files\Tivoli\TSM\Server

**SVCPATH** <TSM server config file path>                      DEFAULT - <same as SVPATH>

### **Specifying TSM server IP port: the SVPORT option**

Use this option to tell AutoVAULT the IP port of the TSM server. Example: SVPORT 1500

**SVIP** [<TSM server ip port>]                      DEFAULT - 1500

### **Specifying action on “tape in use” errors: the TINUSE option**

Use this option to select whether AutoVAULT returns an error if a tape could not be checked out because it was found in use. Example: TINUSE YES

**TINUSE** [YES | NO]                      DEFAULT - YES

### **Specifying a TSM Administrative command to run after AutoVAULT executes: the TSMPCMD option**

Use this option to execute any TSM administrative command after AutoVAULT executes. Multiple TSM commands can be executed by running a TSM Server Script.

**TSMPCMD** <command to execute>                      DEFAULT - None

### **Specifying which TSM version is being managed: the TSMVER option**

Use this option to indicate which TSM Server Version AutoVAULT is managing. Significant TSM database changes were introduced with TSM V6.

**TSMVER** <Integer: 5 or 6>                      DEFAULT - 5

### **Specifying verification of checkout process: the VCEDISABLE option**

Use this option to select whether AutoVAULT should disable verification of a successful media checkout. If set to 'YES', AutoVAULT will issue the command for the media, but will not wait to verify that the command completed successfully. Example: VCEDISABLE NO

**VCEDISABLE** [YES | NO]                      DEFAULT - NO

### **Specifying action on checkout errors: the VCHKOERR option**

Use this option to select whether AutoVAULT should record media as vaulted if the media checkout from the library fails. An error will be listed in the error log and on the tape pull report. If set to 'NO', AutoVAULT will not update the status of the media as offsite. If set to 'YES', AutoVAULT will update the status of the media as offsite. Example: VCHKOERR NO

**VCHKOERR** [YES | NO]                      DEFAULT - NO

### **Specifying web reports: the WEBREPORT option**

Use this option to select whether AutoVault media reports should be created as Storage Manager Scripts so they can be viewed from the TSM web interface. If you have a large amount of offsite media, selecting 'NO' will reduce the amount of activity log entries when AutoVAULT runs. Example: WEBREPORT YES

**WEBREPORT** [YES | NO]                      DEFAULT - YES

## Using the GBMAIL Client

AutoVAULT installs a freeware mail client which you can use to mail reports. It is easy to add this as a post command (see POSTCMD option) run when AutoVAULT execution completes. A sample command file is included in the AutoVAULT installation directory. Rename "avpost\_cmd.smp" to "avpost.cmd" and edit the options.

### Syntax:

```
gbmail [-v] -to <address list...> [-file <filename>] [-h <smtp.server.name>]
[-p <port_number>] [-from <address>] [-cc <address list...>]
[-bcc <address list>] [-s <Subject>] [-t <timeout>]
```

### OPTIONS:

- v     verbose output - more detailed messages.
- file   Name of text file to send as message body.
- h     Name of SMTP server to connect to.  
(If this option is not set, GBMailer will assume 'localhost'.)
- p     Port number for SMTP protocol. (Port is set to 25 by default.)
- from   An optional email address of sender. If not set, GBMailer  
will try to construct an email address by combining the name of the current user and the  
name of local machine. You should set this option in most cases.
- to     REQUIRED   Email address of recipients.  
At least one address must be specified after -to switch.
- cc     (carbon copy) Email addresses of recipients that will be listed in Cc: field.
- bcc    (blind carbon copy) E-mail addresses of recipients that you do not want revealed to  
others receiving the message.
- s     Subject of message.
- t     Timeout for socket operations (in seconds). Set to 300 seconds by default.

### EXAMPLE:

```
gbmail -v -to admin@coderelief.com -file .\reports\tapelist.txt -h mailhost.isp.net
-from tsm@coderelief.com -s "Vault Report"
```

This will email the file "tapelist.txt" to admin@coderelief.com using SMTP server "mailhost.isp.net" with a subject of "Vault Report".

# Troubleshooting

## Error Messages

AV0005	AV0005: AutoVault registry key not found - verify AutoVault installation	The registry entries for AutoVault are missing or invalid. Reinstall AutoVault.
AV0007	AV0007: Multiple license keys are defined and no parm was passed. Execution Ended.	There is no default server if multiple servers are defined. Run autovault.exe with a SERVER= parameter.
AV0008	AV0008: AutoVault parameter error - verify parameter value: <value>	An invalid parameter was passed to the autovault.exe program.
AV0010	AV0010: AutoVault path read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Reinstall AutoVault.
AV0012	AV0012: AutoVault Admin read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Run the AutoVault configurator to specify the TSM administrator userid.
AV0014	AV0014: AutoVault Admin Password read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Run the AutoVault configurator to specify the TSM administrator userid.
AV0016	AV0016: AutoVault Admin key update error	The registry entries for AutoVault could not be updated.
AV0018	AV0018: AutoVault Password key update error	The registry entries for AutoVault could not be updated.
AV0020	AV0020: AutoVault TCPSTServer read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Run the AutoVault configurator to specify the TSM Server Address.
AV0022	AV0022: AutoVault TCPSTPort read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Run the AutoVault configurator to specify the TSM Server Prot.
AV0024	AV0024: AutoVault TCPSTServer key update error	The registry entries for AutoVault could not be updated.
AV0026	AV0026: AutoVault TCPSTPort key update error	The registry entries for AutoVault could not be updated.
AV0028	AV0028: AutoVault License Key is Invalid	The License Key for AutoVault is invalid. Edit the AutoVault license key using the AutoVault License Key Utility.
AV0030	AV0030: AutoVault License Key is valid: <value>	The License Key for AutoVault is valid. If you are running a demo version, the number of days remaining will display.

AV0032	AV0032: AutoVault Demonstration Period has Expired.	The AutoVault trial period has expired. Contact CodeRelief, LLC to purchase AutoVault.
AV0034	AV0034: AutoVault UNIXAdmin read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Reinstall AutoVault.
AV0036	AV0036: AutoVault UNIXPassword read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Reinstall AutoVault.
AV0038	AV0038: AutoVault UNIXPath read error - verify AutoVault installation RC=<value>	The registry entries for AutoVault are missing or invalid. Reinstall AutoVault.
AV0040	AV0040: AutoVault UNIXAdmin key update error	The registry entries for AutoVault could not be updated.
AV0042	AV0042: AutoVault UNIXPassword key update error	The registry entries for AutoVault could not be updated.
AV0044	AV0044: AutoVault UNIXPath key update error	The registry entries for AutoVault could not be updated.
AV0100	AV0100: ADSM registry key not found - verify ADSM client installation	The registry key for the TSM client could not be opened. Reinstall the TSM administrative client.
AV0101	AV0101: ADSM administrative client path not found - verify ADSM client installation	The registry entries for the TSM client are missing or invalid. Reinstall the TSM administrative client.
AV0102	AV0102: ADSM server path not found - verify ADSM server installation	The registry entries for the TSM server are missing or invalid.
AV0103	AV0103: ADSM server registry key not found	The registry key for the TSM server could not be opened. AutoVault is not running on the TSM server.
AV0200	AV0200: ADSM database connection via ODBC failed.	Verify that the TSM ODBC client is installed and configured. Verify that the TSM administrator and password are correct.
AV0210	AV0210: ADSM database ExecuteSQL via ODBC failed.	Verify that the TSM ODBC client is installed and configured.
AV0250	AV0250: SQL call failed <error>	Verify that the TSM ODBC client is installed and configured.
AV0270	AV0270: Unable to create CInternetSession.	Unable to create a session for FTP from a remote UNIX server. Contact Autovault technical support.
AV0272	AV0272: FtpConnection call failed : <error>	Unable to open an FTP session to a remote UNIX server. Contact Autovault technical support.

AV0310	AV0310: ERROR running UPDATE VOLUME command for volume <volume> return code is: <value> .	Verify that the TSM administrator userid and password are correct and the TSM server is available.
AV0320	AV0320: Volume <volser> was in use.	An TSM command was issued for a specific volume and the volume was already in use.
AV0322	AV0322: Skipping volume %s .	AutoVault is skipping a specific volume. It may be in use.
AV0324	AV0324: ERROR running CHECKOUT LIBV command for volume <volume> return code is: <value> .	Verify that the TSM administrator userid and password are correct and the TSM server is available. Possible library hardware problem.
AV0325	AV0325: ERROR running MOVE command for volume <volume>. Review the activity log.	Verify that the TSM administrator userid and password are correct and the TSM server is available. Possible library hardware problem.
AV0326	AV0326: MAXCHECKOUT value of <value> I/O ports exceeded for library <value> while running checkout for volume <value>.	No further media from this library will be vaulted. Empty the I/O ports on the library and rerun AutoVault.
AV0328	AV0328: ERROR running CHECKOUT LIBV process for volume <volume>. Review the activity log.	Verify that the TSM administrator userid and password are correct and the TSM server is available. Possible library hardware problem.
AV0329	AV0329: ERROR running MOVE process for volume <volume>. Review the activity log.	Verify that the TSM administrator userid and password are correct and the TSM server is available. Possible library hardware problem.
AV0330	AV0330: Volume <volume> in skip file and cannot be processed. Manually change status.	You have manually marked this volume for exclusion. Run the Return Media GUI and remove the skip flag.
AV0400	AV0400: VAULT.OPT invalid option value - errlog.	The errlog option in the vault.opt option file contained an invalid value. Defaults to 30.
AV0410	AV0410: VAULT.OPT invalid option value - dbcycle.	The dbcycle option in the vault.opt option file contained an invalid value. Defaults to 5.
AV0500	AV0500: Printing requested but no default printer is defined.	Define a default printer.
AV0600	AV0600: Cannot copy server files for recovery.	Recovery script creation is incomplete. Verify that AutoVAULT is running on the TSM server.
AV0610	AV0610: Device Configuration File is not defined.	Recovery script creation is incomplete. Define a device configuration file on the TSM server.
AV0620	AV0620: Volume History File is not defined.	Recovery script creation is incomplete. Define a volume history file on the TSM server.
AV0640	AV0640: Error opening ftp connection to UNIX server.	Run AutoVAULT configuration and verify UNIX userid and password. Userid must have ftp access to UNIX Storage Management Server.

AV0642	AV0642: Ftp of dsmserv.opt from UNIX server failed.	Ftp of file from UNIX Storage Management Server failed. Verify ftp userid has access to the file and the file exists.
AV0644	AV0644: Ftp of volhist from UNIX server failed.	Ftp of file from UNIX Storage Management Server failed. Verify ftp userid has access to the file and the file exists.
AV0646	AV0646: Ftp of devconfig from UNIX server failed.	Ftp of file from UNIX Storage Management Server failed. Verify ftp userid has access to the file and the file exists.
AV0910	AV0910: Unable to open file: <file handle>	AutoVault was unable to open a file. Refer to the program output and the error report for more detailed messages.
AV0912	AV0912: Recoverable file open error cleared: <file handle>	AutoVault received a recoverable error opening a file. Refer to the program output and the error report for more detailed messages.
AV0920	AV0920: No errors were encountered.	AutoVault ran successfully without errors.
AV0921	AV0921: Errors were encountered.	AutoVault run completed with errors.
AV0922	AV0922: Auto Vault version 1.1.0 started.	AutoVault execution started.
AV0924	AV0924: AutoVault execution ended. RC=<value>	AutoVault execution ended.
AV0930	AV0930: Error log purged. Lines processed: <value> Lines deleted: <value>	AutoVault informational message. No action required.
AV0931	AV0931: Badline - <value>	AutoVault corrected an invalid line in the error log. No action required.
AV0999	AV0999: AutoVault execution abnormally terminated: <function>	The AutoVault program terminated prematurely with errors. Refer to the program output and the error report for more detailed messages.

## Known Problems

**EXCESSIVE CONNECTION MESSAGES - IBM APAR IC33963** - When running AutoVAULT interactively using the TSM v5.1 ODBC interface, an excessive number of TSM connection messages are issued to the AutoVAULT console. If you are running AutoVAULT manually, use the latest TSM v5 ODBC Driver, v5.1.1.1 or higher.

**ODBC ERRORS - ODBC error IM004.** Update your version of Microsoft MDAC to the latest version.

**ODBC Client Missing** - The Tivoli Storage Manager clients do not install the ODBC interface by default. Download the TSM ODBFC client separately from the IBM ftp site and install.

**SCHEDULER SYNTAX** - When scheduling AutoVAULT to run with the TSM scheduler from a path that contains a space, enclose the entire path in both single and double quotes. For example, to run from the default path you would schedule an TSM backup/archive command action with an object of "C:\Program Files\AutoVAULT\AutoVAULT.exe". Note that subsequent edits of this schedule may remove the outer single quotes. Therefore, verify that the path is enclosed first in double quotes then in single quotes after every edit. A preferred method is to schedule the command object as c:\progra~1\AutoVAULT\AutoVAULT.exe. This eliminates all embedded spaces.

**PRINT FROM A SERVICE** - The Windows system account does not have a default printer. If you would like reports printed, you must run the Storage Manager scheduler from a userid with a default printer defined. Note that if you are also running backups from this service, the userid must have the proper authority for the server. A user with administrator authority is recommended.

## Technical Support

### **Basic Support (Included free for the first year) Annual maintenance required**

Basic Support gives you email and phone access to Code Relief Technical Support, with guaranteed response within 24 hours on business days (Monday-Friday). Free product upgrades are also included. Basic Support is free for the first full year after purchase. After the first year, there is an annual fee (currently 15% of the AutoVAULT list price). To protect yourself from price increases and to ensure uninterrupted coverage, you may order multiple years of support in advance.

Email problems and questions to [tech@coderelief.com](mailto:tech@coderelief.com).

Please include:

- Your AutoVAULT product license key or indicate that you are running a trial version.
- Your name, company, email, and phone number.
- A description of the problem
- All trace files (<install path>\debug\trace\*.txt)

*Most AutoVAULT customers rarely need additional support. Due to the low frequency, we offer the following 24x7 support to assist customers in special times of need.*

### **Planned Disaster Testing Support - \$150 per hour**

Code Relief offers 24-hour support for planned disaster tests. You should order this service (with a credit card or faxed purchase order) at least 30 days prior to the test. The specific date and hours when our support will be needed must be noted. A fee of \$150 per hour (in .25 hour increments) will be charged for the support received during the time range requested. For example: If the test is scheduled from 5 PM to 9 PM and Code Relief Technical Support is used from 8 PM to 8:30 PM, the fee will be \$75 (\$150 x .5). Support received outside the requested time range will be billed at the Emergency Support rate of \$250 per hour (in .25 hour increments).

### **Emergency Support - \$250 per hour**

To access this service, you must call 1-610-926-2556 and choose the Emergency Support menu option for current instructions and emergency phone number. A Code Relief technician will respond within 2 hours. When calling for this service, a credit card number or faxed purchase order (valid one business year from issue date) must be provided. 24/7 Emergency Support is charged at a rate of \$250 per hour (in .25 hour increments).

# Index

## A

Abnormal Termination.....	8
Active Data Pools .....	56
Additional Settings.....	32
administrative ID and Password .....	22
AUDIT Log for media movement .....	44
AUDITLOG option.....	51
AutoVAULT License Key .....	17

## B

Backup of AutoVAULT .....	38
BKSVault option .....	51

## C

Checking in Media.....	41
Checkpoint Recovery.....	8
Client Node Disaster Recovery Instructions.....	38
Configuring AutoVAULT .....	21
Copy Storage Pools.....	27
COPYPOOL option .....	51

## D

Database and Backup Set Options .....	31
DBBVAULT option.....	51
DBCYCLE option.....	52
DBSCYCLE option .....	52
DBSVault option.....	52
Disaster Recovery .....	15
Disaster Recovery Instructions Example .....	47
Disaster Recovery Script Details .....	46
Disaster Recovery Scripts-Customizing .....	46
Disaster Recovery Scripts-Vaulting.....	46
DRM Vaulting Method.....	23
DRMUSE option.....	53

## E

Emailing Reports .....	61
Emailing the AutoVAULT Reports .....	38
ERRLOG option .....	53
Error Messages.....	65
Excessive ACTLOG Messages.....	66

## F

FTP media reports to a vaulting company .....	45
FTPERROR option .....	53
FTPPASSIVE option .....	53

## G

GBMAIL client.....	61
Gresham EDT-Distributape .....	41

## I

Installation Checklist .....	20
Installing and Upgrading AutoVAULT .....	17
Interface files created by AV .....	44
Iron Mountain .....	45
ISERVER option.....	53

## L

Library Clients .....	23
Library Configuration .....	30
LIBRARY option.....	54
License Keys-AutoVAULT.....	17

## M

Manual Execution .....	43
Media Totals .....	8
Message Suppression in TSM.....	44
MODE option .....	55
Moving AutoVAULT to a new location.....	38
Multiple TSM Servers - Adding more TSM Servers.....	19
Multiple Vault Locations .....	11

## O

ODBC Data Source.....	24
ODBC ERRORS .....	66
ONSITECHK option .....	55
Overview.....	15

## P

Parameter input .....	42
Post TSM Administrative Command.....	59
POSTCMD option .....	55
PRECMD option.....	56
Primary Storage Pools .....	28
PRIMARYPOOL option .....	56
PRINT FROM A SERVICE .....	66
Printing AutoVAULT reports.....	37
PRINTRPT option .....	56
Problems .....	66

## Q

QWIKSCAN option.....	57
QwikScan™ Interface.....	41

## R

Remote Access to AutoVAULT .....	41
Remote TSM Server Information .....	25
Requirements for AutoVAULT .....	13
Returning Media .....	40
REUSEDELAY option .....	57
RHPULL option.....	57
RHRETURN option.....	57
RHVAULT option .....	57
RPTHEAD option.....	58
RPTORDER option .....	58
RPTSELECT option .....	58
Running AutoVAULT .....	36

## S

SCHEDULER.....	66
SECURITY option.....	58
SERVER= Parameter.....	42
SVCPTH option .....	59
SVFTPPATH option.....	58
SVIPOption.....	59
SVPATH option.....	59
SVPORT option.....	59

## T

Technical Support .....	67
Test Mode - READONLY .....	23
TINUSE option .....	59
Traditional Vaulting Method .....	23
Troubleshooting .....	66
TSM Server Information.....	22
TSM Server Versions.....	60
TSM Version 6.....	23
TSMPCMD option.....	59
TSMVER option .....	60

## U

Upgrade Considerations.....	12
-----------------------------	----

## V

Vault Location Changes.....	45
vault.opt file .....	51
Vaulting company - automating daily operations .....	45
VCEDISABLE option .....	60
VCHKOERR option .....	60
Vital Records, Inc. ....	45

**W**

<b>WEBREPORT option .....</b>	<b>60</b>
<b>What's new in AutoVAULT V2.....</b>	<b>11</b>
<b>What's New in AutoVAULT V3.0.....</b>	<b>9</b>
<b>What's New in AutoVAULT V3.3.....</b>	<b>8</b>
<b>Windows Server Instance - Selecting .....</b>	<b>26</b>