

Altiris Recovery Solution™ 7.0
from Symantec
Implementation Guide

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Altiris and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION, INCLUDING WITHOUT LIMITATION ITS AFFILIATES AND SUBSIDIARIES, SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation," as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display, or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<http://www.symantec.com>

Document Date: July 1, 2009

This product includes software developed by the Apache Software Foundation. Such software is subject to the below conditions.

The Apache Software License, Version 1.1

Copyright (c) 1999-2004 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Xerces" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright (c) 1999, International Business Machines, Inc., <http://www.ibm.com>. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Contents

Chapter 1: Introducing Recovery Solution	8
About Recovery Solution	8
How Recovery Works	9
How the Temporary Operating System Is Created	9
Where to get more information	10
Chapter 2: Planning and Technical Information	12
Product Limits	12
Recovery Disk Space Needed	13
Performance Tips	13
Re-indexing the Recovery Database	13
Data Protection Performance	13
Restore Performance.	14
Changing DCOM Protocols	15
Configuring Microsoft Network Load Balancing	16
Settings Information.	16
User Account and Share Configuration	17
Shared Folders.	19
Microsoft SQL Server Settings	19
Event Log Configuration	21
Internet Information Server Configuration	21
ODBC Configuration	25
DCOM Configuration	26
RPC Dynamic Port Allocation	30
Firewall Configuration	31
Web-Based File Recovery Configuration	31
Configuring Web-Based File Recovery to run on Windows Server 2003	34
Protected Computer IP Address Updates	34
Job Schedule Worksheet	35
Chapter 3: Installing Recovery Solution	37
About Recovery Solution requirements	37
Setting up Recovery Solution prerequisite components	37
Configuring the load balancer	38
About installing Microsoft Network Load Balancing	38
About configuring the BIG IP Controller Health Monitors	38
Configuring the SQL Database	40
Discovering computers	40
Installing the Altiris Agent	40
Installing the Recovery Solution product	41
After Server Installation Is Complete	41
Upgrading Recovery Solution	42
Upgrading Recovery Clusters	43
Upgrading Recovery Servers	43
Upgrading Recovery Agents	44
Licensing Recovery Solution.	44
Uninstalling Recovery Solution	45
Uninstalling the Recovery Agents	45

Uninstalling Recovery Servers	45
Uninstalling Recovery Clusters	46
Chapter 4: Command Line Utilities	47
AeXRSEnc Utility	47
AeXMigrt.com Utility	50
Overview	50
Command-line parameters.	52
Input XML files	54
Chapter 5: Recovery Solution Infrastructure Backup and Restore.	57
Recovery Solution Infrastructure	57
Backup	57
Notification Server Database Backup.	58
Recovery Database Backup	59
Data Files Backup	60
Load Balancer Configuration Backup and Restore	61
Restore	61
Notification Server Database Restore	62
Data Files Restore	62
Recovery Database Restore	62
Chapter 6: Recovery Agent Troubleshooting	64
Troubleshooting: Install/Uninstall	64
Troubleshooting: Cannot Update Recovery Agent	64
Troubleshooting: Settings Not Saved During Update.	65
Troubleshooting: Install fails with unable to configure the settings error	65
Troubleshooting: Snapshots.	65
Troubleshooting: Snapshot Options Unavailable	66
Troubleshooting: Nothing Happens	66
Troubleshooting: Erratic Behavior	67
Troubleshooting: Snapshots Don't Run	67
Troubleshooting: Scheduled or Automated Snapshot Doesn't Run	67
Troubleshooting: Snapshot on Logoff Doesn't Run	68
Troubleshooting: Snapshot Stops Prematurely	69
Troubleshooting: Recovery Solution Stops During a Snapshot or Restore	69
Troubleshooting: Windows Installer Appears During Snapshots	70
Troubleshooting: Snapshot Is Missing Files	70
Troubleshooting: Restoring Data	71
Troubleshooting: File Restores	71
Troubleshooting: Cannot View Protected Files	72
Troubleshooting: Protected File Versions	72
Troubleshooting: Cannot Find File Versions	72
Troubleshooting: Protected File Versions Are the Same	72
Troubleshooting: Not Enough Space Available to Restore (FAT32)	73
Troubleshooting: Miscellaneous File Version Problems.	73
Troubleshooting: Web-Based File Recovery Logon Doesn't Appear	73
Troubleshooting: Restore Crashes Windows Explorer	73
Troubleshooting: Recovery Solution Freezes During File Search	74
Troubleshooting: Restore Stops Prematurely	74
Troubleshooting: Unknown Restore Type.	74
Other Issues Relating to Restoring Data	74
Custom user names for message queues gets renamed into the GUID-like names	74
Troubleshooting: Error Messages	75

Troubleshooting: Error Messages in the Progress Dialog Box	75
Troubleshooting: New Error	75
Troubleshooting: Repeated Error	76
Troubleshooting: Error Message Boxes	76
Troubleshooting: Job Could Not Be Submitted	77
Troubleshooting: Drive Configuration Message	77
Troubleshooting: System Low on Registry Quota	77
Troubleshooting: Options	77
Troubleshooting: Can't Open Options	78
Troubleshooting: Options Are Unavailable	78
Troubleshooting: Schedule Settings Cannot Be Displayed	78
Troubleshooting: Event Logs	79
Troubleshooting: Event Log Full	79
Troubleshooting: Error Messages in the Event Logs	79
Troubleshooting: Error Checklist	79
Troubleshooting: Rollback	79
Troubleshooting: Virus Warning During Rollback	80
Troubleshooting: Rollback Has Missing or Damaged Files	80
Troubleshooting: Rollback Disables Computer	81
Troubleshooting: Rollback General Protection Fault Error Message	81
Troubleshooting: DHCP Problems After Rollback	81
Troubleshooting: Other Issues	81
Troubleshooting: Cannot perform user registration or authentication	82
Troubleshooting: DCOM	82
Troubleshooting: FrontPage 98 Personal Web Server Conflict	82
Troubleshooting: Logon Problems	83
Troubleshooting: Cannot Access Dialog Box Buttons	83
Troubleshooting: Connection Firewall	84
Troubleshooting: Fast User Switching	84
Troubleshooting: Unknown Solution	84
Troubleshooting: Event Viewer	84

Chapter 7: Recovery Solution Troubleshooting 85

Where to look for troubleshooting information	85
About Recovery Solution event logs	85
Viewing events	86
Recovery Solution installation troubleshooting	86
Server installation troubleshooting	87
After installation, W3SVC warnings appear in System event log	87
If Recovery Server uninstall encounters an error, uninstall rollback may fail	87
Altiris Recovery Server service error message after completing a Recovery Server upgrade	87
Recovery Server upgrade hangs with "Upgrade in progress" status forever	88
Recovery Solution tasks are non-factional after aggregation of legacy servers	88
Altiris Recovery Server cannot be installed because 8.3 file names creation is disabled	88
Troubleshooting user installations	89
Error message appears during Recovery Agent setup	89
User account not validated	89
Setup does not run properly	90
Applications will not start after agent install	91
User account & logon troubleshooting	91
Protected Computers Cannot Connect to Server	91
User Logon Issues	92
Protected users cannot be authenticated	93
Data protection & recovery troubleshooting	93

Snapshot & File Restore Troubleshooting	93
Snapshot schedule for certain computers do not run.	93
User cannot log on to start snapshot.	94
Job cannot be submitted	94
Protected computer drives missing from snapshots.	94
User cannot browse protected files	94
User cannot access a different account via web-based file recovery	94
Snapshots fail because server clocks are not synchronized	95
General snapshot & recovery problems	95
Full System Recovery troubleshooting.	95
Disk space error appears during Full System Recovery disk creation.	96
Full System Recovery does not start properly	96
Error appears during Full System Recovery	96
Full System Recovery fails when creating disk structure	99
Full System Recovery incomplete, but no error appears	99
Problems occur after server upgrade.	100
Recovery Agent not working after Full System Recovery	101
Files missing or outdated after Full System Recovery	101
Full System Recovery stalls	101
Full System Recovery CD-ROM failure	101
Cannot cancel restore of folder.	102
Account disabled after full system recovery	102
Full System Recovery fails on HP NetServer LC2000	102
Rollback troubleshooting	102
Unable to see desired snapshot during a system rollback	102
Rollback cannot be started from the console	103
Job cannot be submitted	103
After rollback, user is prompted to uninstall.	103
Rollback fails	103
After rollback, a restored drive contains no data.	104

Appendix A: Hard Disk Support. 105

Index. 106

Chapter 1

Introducing Recovery Solution

This chapter includes the following topics:

- [About Recovery Solution](#) (page 8)
- [How Recovery Works](#) (page 9)
- [Where to get more information](#) (page 10)

About Recovery Solution

Recovery Solution protects operating systems, applications and data stored on desktops and notebooks from unintentional changes, accidental deletions, and catastrophic loss from hardware failure, virus corruption, or theft. By taking daily snapshots automatically, the solution works seamlessly and unobtrusively to protect your systems and data without impacting user productivity.

Recovery Solution provides total and system-wide protection for your organization's computers, including operating system, applications, network settings, drive mappings, peripheral drivers, data, and other configuration settings. Recovery Solution captures e-mail messages, contacts, and calendar entries, even while the e-mail application is in use. Users can work completely unaware that snapshots are being taken. Remote users are prompted at login to allow the snapshot, but once it begins, the process is transparent and users can continue with their work uninterrupted.

Recovery Solution provides a three-level approach to minimize bandwidth and CPU utilization with each snapshot:

- Redundant File Elimination (RFE): Patented technology filters out files that already exist in the Altiris recovery repository, storing common files once across your entire organization (Recovery Solution only).
- Redundant Block Elimination (RBE): Patented technology that reduces data transmission size by transmitting and storing only the portions of each file that is different from the previous snapshot.
- HLZS data compression is the industry standard for lossless data compression.

These technologies work together to make the backup process as seamless and efficient as possible, and achieve compression ratios as high as 15:1, minimize network and CPU loads, and provide scalability to thousands of users per repository.

Note

For a list of new features for Recovery Solution 7.0, see the *Recovery Solution Release Notes*.

How Recovery Works

Restoring a file from the cluster is as simple as dragging and dropping the file to its destination.

When a user restores a file, Recovery Solution does the following.

1. Determines if the copy of the file being recovered is different from the copy that already exists on the user's computer. If a user recovers an entire folder. Example: it is possible that some of the files it contains have not changed and do not need to be transferred from the server.
2. If the file needs to be copied, determines if the file was originally obtained from that user's computer, or if the snapshot just contains a placeholder with information about where an identical file is stored. Remember that Recovery Solution includes each file in a snapshot only once.

If a placeholder was used during the snapshot, Recovery Solution locates the actual file.

3. Decompresses the file and copies it to the protected computer.

During this process, Recovery Solution reconstructs the file if more than one version was included in a snapshot. Since the file was copied in its entirety only for the baseline snapshot, restoring a later version means assembling the pieces of the file that were copied during the baseline and during subsequent snapshots. The file is constructed as the pieces are downloaded.

Files are reconstructed quickly, so there is usually little time difference between Recovery Solution restore and a simple file copy.

Recovery Solution does all of these things automatically. If a user restores an entire folder or a drive, Recovery Solution performs these actions for each restored file. The result is that the user gets complete copies of restored files as they were at the time of a snapshot.

You can also use either rollback or Full System Recovery to return the files on the computer to their state at a selected point in time. This can be useful to reverse unwanted changes to the operating system and other important files. Users can also perform rollbacks themselves.

Specific files can also be restored from Full System Recovery CD-ROMs if the protected computer is bootable. This can be useful if a remote user is not on the local network and needs to restore files quickly. A Full System Recovery CD-ROM can be password-protected, in which case an Recovery Solution user name and password are required to access the files on the CD-ROM. For more information on password-protection and access to CD-ROM data, see "Creating Full System Recovery disk" in the *Recovery Solution User's Guide*.

How the Temporary Operating System Is Created

Every time a protected computer starts, a system file installed with Recovery Solution monitors which files are accessed during the startup process. This is the File Access Logger, or FAL, and it creates a log that contains the list of startup files. A corresponding FAL Stopper, which appears as a service under Windows 2000/XP, stops the FAL as soon as Windows has finished starting up. When a Full System Snapshot is performed, the FAL log is sent to the server and stored along with the protected files.

When you create Full System Recovery disks, Recovery Solution also creates a temporary operating system from this list of startup files and stores a compressed copy of this operating system in a CD-ROM image. When compressed, a small temporary operating system image uses about 20 MB of disk space, but depending on the protected computer's configuration it is possible to have a much larger image. For a Windows 2000 computer, you will typically need about 100 MB.

Where to get more information

Use the following documentation resources to learn and use this product.

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as article 41188 in the Altiris Knowledge Base.	https://kb.altiris.com/article.asp?article=41188&p=1
Implementation Guide	(This guide) Information about how to install, configure, and implement this product. This information is available in PDF format.	The Documentation Library and Product Support page, which is available at the following URLs: <ul style="list-style-type: none"> • http://www.altiris.com/support/documentation.aspx • http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the Documentation link on the right side of the page.

Document	Description	Location
Recovery Solution User's Guide	<p>Information about how to use this product, including instructions for performing common tasks.</p> <p>This information is available in PDF format.</p>	<ul style="list-style-type: none"> • The Symantec Management Console's Documentation Library, which is available in the Symantec Management Console on the Help menu. • The Web-based documentation library, which is available at the following URL: http://www.altiris.com/support/documentation.aspx • The Product Support page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the Documentation link on the right side of the page.
Help	<p>The same content as the User's Guide, but in HTML help format.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p>	<p>The Documentation Library, which is available in the Symantec Management Console on the Help menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <ul style="list-style-type: none"> • The F1 key • The Context command, which is available in the Symantec Management Console on the Help menu.
Recovery Agent User's Guide	<p>Information for endpoint users about how to use the Recovery Agent on client computers.</p> <p>This information is available in PDF and Help format.</p> <p>This information is also included in the Recovery Solution documentation.</p>	<p>Installed with the Recovery Agent in PDF and Help formats.</p>

Chapter 2

Planning and Technical Information

This section contains additional information about Recovery Solution.

- [Product Limits](#) (page 12)
- [Recovery Disk Space Needed](#) (page 13)
- [Performance Tips](#) (page 13)
- [Settings Information](#) (page 16)
- [Protected Computer IP Address Updates](#) (**page 34**)
- [Job Schedule Worksheet](#) (page 35)

Product Limits

Listed below are some of the known limits of Recovery Solution.

- **Data Protection & Recovery Limits**

The following restrictions apply to snapshots.

- Recycle Bin files are automatically excluded from all snapshots. You cannot change this option.
- A maximum of 32767 versions of any one protected file can be stored on the cluster.

- **Full System Recovery Limits**

The following restrictions apply to Full System Recovery.

- Full System Recovery cannot be performed on a protected computer running disk compression software (such as DriveSpace or Stacker).
- GUID Partition Table partitions are not supported. A Full System Recovery collection fails.

- **Maximum number of threads**

When HTTP transport protocol is used, the maximum number of threads that a Recovery Server can process is 32 per each CPU. If the number of currently running snapshots is higher than the number of CPU cores on the server multiplied by 32, the Recovery Agent on client computers starts losing the connection to the Recovery Server. To avoid this situation, the HTTP threads count should be manually increased through the registry.

The following registry value should be added.

Under the registry key [HKEY_LOCAL_MACHINE/SOFTWARE/Altiris/eXpress/Client Recovery], add DWORD value "HttpVault_ThreadCount" equal to the total number of threads you'd like to be processed by Recovery Server when HTTP transport protocol is used. You need to restart IIS and Recovery Server services to apply changes.

Recovery Disk Space Needed

In general, to recover a file a protected computer must have at least the size of the recovered file in free disk space.

However, this rule might not suffice in all situations. Redundant Block Elimination, which minimizes the amount of disk space needed to store multiple versions of protected files, also requires a little extra disk space on the protected computer for recovering files. If there is not enough free disk space, the user encounters an error when attempting to recover the file.

The actual calculations for the amount of disk space needed are somewhat involved, but if you have an idea about how big the earlier versions of a file have been, you can at least determine the maximum amount of space that would be needed to recover the file.

To calculate the maximum amount of recovery disk space required

1. Determine the largest size that the file has been since it was first protected.

If multiple files are being recovered as one job, determine the largest size that any one of the recovered files has been since it was first protected.

Since files increase in size more frequently than they decrease, in many cases the size of the version being recovered is an adequate estimate of the largest file size.

Example: Suppose 3 files are being recovered, with file sizes 200 KB, 250 KB, and 100 KB. If the 250 KB file has always been the largest file, and it was once 400 KB at the time of a snapshot, then use 400 KB as an estimate of the largest file size.

2. Add the sizes of any remaining files being recovered.

Example: To 400 KB, add the sizes of the other two files (200 KB and 100 KB). The total amount of disk space needed to recover the files is 700 KB.

Performance Tips

Though not required to use Recovery Solution, the following information could help you get better performance from the product.

The following topics are covered in this section:

- [Data Protection Performance](#) (page 13)
- [Restore Performance](#) (page 14)
- [Changing DCOM Protocols](#) (page 15)
- [Configuring Microsoft Network Load Balancing](#) (page 16)

Re-indexing the Recovery Database

Over time, the Altiris Recovery Database can become very fragmented (more than 95% for some tables). For information, see the following article:

<https://kb.altiris.com/article.asp?article=45841&p=1>

Data Protection Performance

Following are some tips you can use to ensure that snapshots run efficiently.

- You can help to improve the speed of baseline snapshots by seeding the cluster with files that exist on most users' computers. Since Recovery Solution checks for the existence of each file on the cluster and only transfers it if it is not already there, seeding the cluster with common operating systems, programs, and other files can reduce the amount of time that the initial snapshot takes for most or all protected computers.

Seed the cluster just after you set it up, and before allowing users to take a snapshot. Many of the files being protected will then already exist on the cluster.

Here are some examples of files you might want to initially add to the cluster.

- Windows Vista, Windows XP, Windows 2000 installations.
- Applications used throughout your company, particularly those that take up moderate to large amounts of disk space. Common examples are Microsoft Office, Microsoft Internet Explorer, Netscape Communicator, and Lotus Notes.
- Common data files that might reside on many users' hard disks.

If you seed the cluster with multiple protected computer installations, you should perform snapshots one at a time, allowing each one to complete before starting the next one. That way you are sure to get the maximum benefit from Redundant File Elimination and Redundant Block Elimination.

- Try to avoid having a remotely connected computer be the first one to protect any particular application. Instead, protect a computer on the network that has this application installed to eliminate the need to transfer the application over a slow link.
- If snapshots are exceptionally slow for protected computers running Windows 2000/XP, you might benefit from changing the primary DCOM protocol being used for communications. For more information, see [Changing DCOM Protocols](#) on page 15.
- If you are using Microsoft Network Load Balancing with Recovery Solution, snapshot performance can be improved by appropriately configuring your Network Load Balancing Cluster settings. For more information, see [Configuring Microsoft Network Load Balancing](#) on page 16.
- If your protected computers use HTTP protocol for communication with Recovery Server, you can improve the performance of jobs on clients running Windows 2000, by clearing the **Enable Integrated Windows Authentication (requires restart)** checkbox in Windows Control Panel > Internet Options > Advanced tab > Security on client computers. In this case, a less secure (but more robust) NTLM protocol will be used for authentication with the server.

Restore Performance

Following are some tips you can use to ensure that recoveries run efficiently.

- Over a dial-up connection, it is practical to restore up to a few tens of megabytes. For larger file sets, or for Full System Recovery, it makes more sense to ship user data on CD-ROM to the remote location. Alternatively, you can send the protected computer to a place where it can be connected at high speed to the server, and restore the data from there.
- If recoveries are exceptionally slow for protected computers running Windows 2000/XP, you might benefit from changing the primary DCOM protocol being used for communications. For more information, see [Changing DCOM Protocols](#) on page 15.

Changing DCOM Protocols

Most of the data transferred back and forth between protected computers and the server is sent via Microsoft Distributed Component Object Model (DCOM). DCOM itself employs RPC (remote procedure call) to actually send messages from one networked computer to another.

When running on Windows 2000/XP, DCOM can be configured to use any of several different RPC network protocols to send and receive messages. By default, Windows uses UDP (commonly known as datagram packets) protocol. UDP typically uses less network bandwidth and is quicker than TCP—unless packets start getting lost regularly. Since UDP is a connectionless protocol, DCOM itself handles the retransmitting of packets that fail or become lost. If the network is busy or has other problems that cause a number of DCOM packets to get lost, then data transfer rates can become very slow because DCOM has to retransmit a large number of packets. This can greatly impact the performance of snapshots and recoveries.

To improve performance in these situations, you can configure a protected computer to use TCP as its primary DCOM protocol.

To configure DCOM to use TCP as its primary protocol

1. On the protected computer, from the Windows **Start** menu, click **Run**.
2. Enter DCOMCNFG.EXE.
3. Do one of the following:
 - Change the list of DCOM protocols used specifically for Recovery Solution. This is safer than changing the default DCOM protocols for the entire system. However, it involves a few more steps, and if Recovery Agent is ever uninstalled and reinstalled on the protected computer, the changes are lost and must be made again.

To change the list of protocols for Recovery Solution, do the following.

- a. On the **Applications** tab, in the **Applications** list, select **Altiris Recovery Agent**.
- b. Click **Properties**.
- c. Click **Endpoints**.
- d. Click **Add** to add all missing protocols except **Connection-oriented TCP/IP** to the **DCOM Protocols and endpoints** list.

This helps to ensure that a connection can be established even if something goes wrong with the TCP/IP communications.
- e. If **Connection-oriented TCP/IP** appears in the list but is not at the top, select it and click the **Remove** button. This is the only way to change its position in the list.
- f. If **Connection-oriented TCP/IP** does not appear in the list, add it to the list as follows.
 - Click **Add**.
 - In the Protocol Sequence list, click Connection-oriented **TCP/IP**.
 - Click **OK**.
 - Click **OK** to accept the changes.

- Change the default list of DCOM protocols for the entire system.
Changing the default protocols for the system might give you similar advantages for other applications, but it might also cause problems for other applications that use DCOM and must use UDP for communications. In most cases, however, it should not matter which protocol is used.

Example

To change the list of default protocols, do the following:

- g. Click the **Default Protocols** tab.
 - h. In the **DCOM Protocols** list, look for the item Connection-oriented TCP/IP.
If you do not see it, add it to the list as follows.
 - Click **Add**.
 - In the Protocol Sequence list, click **Connection-oriented TCP/IP**.
 - Click **OK**.
 - i. In the **DCOM Protocols** list, select **Connection-oriented TCP/IP**.
 - j. Click the **Move Up** button repeatedly until **Connection-oriented TCP/IP** is at the top of the list.
4. Click **OK** to save the changes and exit Distributed COM Configuration Properties.
 5. Restart the computer.

Configuring Microsoft Network Load Balancing

If you are using Microsoft Network Load Balancing with Recovery Solution, you can configure your Network Load Balancing cluster properties to improve snapshot performance as follows.

1. Open Network Load Balancing Manager console for your cluster through Windows **Start** menu > **Control Panel** > **Administrative Tools**.
2. Right-click cluster name in the Network Load Balancing Clusters list on the left and select **Cluster Properties** from the drop-down menu.
3. In the **Cluster Properties** dialog window on the **Port Rules** tab select the Defined port rules for Recovery Solution and click the **Edit** button to open the **Add/Edit Port Rule** dialog window.
4. Set **Affinity** to **Single** in the **Filtering mode** section.
5. Click **OK** to save the settings and close the **Add/Edit Port Rule** dialog window.
6. In the **Cluster Properties** dialog window go to **Cluster Parameters** tab and set **Cluster operation mode** to **Multicast**.
7. Click **OK** to save settings and exit Network Load Balancing Manager.

Settings Information

This section contains additional information about settings created and used by Recovery Solution.

- [User Account and Share Configuration](#) (page 17)

- [Microsoft SQL Server Settings](#) (page 19)
- [Event Log Configuration](#) (page 21)
- [Internet Information Server Configuration](#) (page 21)
- [ODBC Configuration](#) (page 25)
- [DCOM Configuration](#) (page 26)
- [RPC Dynamic Port Allocation](#) (page 30)
- [Firewall Configuration](#) (page 31)
- [Web-Based File Recovery Configuration](#) (page 31)
- [Job Schedule Worksheet](#) (page 35)

User Account and Share Configuration

During Setup, Recovery Server creates Windows users and shared folders as needed to simplify deployment and to allow the server to communicate with the protected computers. Automated Account Configuration

Recovery Solution automatically creates the following user accounts and groups.

Account Configuration

Account or Group	Description
XUSR_RepNDM User Account (Local)	<p>Recovery Solution requires this special account for communicating (via DCOM) between the server and the protected computers. This account is given the minimum default rights assigned to users; it requires only the Access this computer from the network right to be used by Recovery Solution. The account is created locally on the server, so it cannot be used to access other computers on the domain. All the required accesses are configured through DCOM.</p>
AeXRS_Users User Group (Local)	<p>This group is given the access rights to protect and restore files with Recovery Solution. You can change its name during Recovery Server Setup, but not thereafter.</p> <p>By default, this group contains the Domain Users group, which means that all domain users have the necessary rights to protect their computers.</p> <p>Notes</p> <p>If you have users on trusted domains that you want to be able to use the server, you must add those users to the Domain Users group for the server or the AeXRS_Users group before they can use Recovery Solution.</p> <p>If the server is installed using local server security, this user group is granted the Log on locally right on the server, which is required for access to Web-based file recovery. If you do not intend to use Web-based file recovery, you can remove this right through Windows.</p> <p>If you want to restrict access to certain individual users, you will have to remove Domain Users from AeXRS_Users. Windows domains allow different types of user groups, including <i>local</i> and <i>global</i>. Because of the way the Windows security model works, you can simplify administration tasks by using a combination of local and global groups. Global groups can only contain users, but local groups can contain both users and global groups. For granting access, we recommend that you create a new global group in the domain, add the users to the global group, and then add the global group to the local group AeXRS_Users.</p> <p>This strategy offers you maximum flexibility in more complicated situations—you get the ease of managing a global group for the individual users combined with the ease of adding other entire groups to the local AeXRS_Users group as appropriate. Example: if you begin your deployment by allowing access to a select group of pilot users (by creating a global group of those users and adding it to the AeXRS_Users local group), you can then easily expand by allowing access to one department at a time, simply by adding their department global groups to the AeXRS_Users local group.</p>

Account Configuration (Continued)

Account or Group	Description
AeXRS_Managers User Group (Local)	This group is given the rights to restore data for any client using the Migrate utility and Web-Based File Recovery.
Altiris Helpdesk Technicians User Group (Local)	Members of this group have rights to perform certain Recovery Solution tasks through the Altiris Console.

Shared Folders

Recovery Server Setup automatically creates a folder for Recovery Agent installation files and shares it so that users can easily install the software from this folder. By default, the folder is stored within the server program files folder.

Microsoft SQL Server Settings

Recovery Server Setup automatically configures Microsoft SQL Server. Following is a list of the changes that are made.

Performance Enhancements

Currently, Recovery Server Setup changes only the **Max Worker Threads** setting from its default. This change is based upon our experiences in two sets of early Beta deployments of the product.

Max Worker Threads

Configures the number of worker threads that are available to SQL Server processes. SQL Server makes use of the native thread services of the operating system. Instead of one worker thread, there are many. Each network that SQL Server simultaneously supports is supported by one or more threads, another thread handles database checkpoints, and a pool of threads handles all users.

The max worker threads option allows you to control the number of threads allocated to the user pool. When the number of user connections is less than max worker threads, one thread handles each connection. However, if the number of connections exceeds max worker threads, thread pooling occurs. Additionally, if the configured value for worker threads is exceeded, the request is handled by the next worker thread that completes its current task. The default is 255.

—Microsoft Transact-SQL Reference

Additional Information

A worker thread performs a database operation on behalf of a client. While it may seem that one thread per connection is ideal for performance, an excessive number of threads will cause the server to spend more time simply managing the threads and can result in significant contention for CPU time among the threads. In a 1996 Compaq TPC-C benchmark with SQL Server 6.5 running on Windows NT 4.0, the optimal setting for **max worker threads** was **100**, even with 5000 concurrent users.

Databases

Setup creates and configures databases as follows.

- **Recovery Database**

The default name for this database is AeXRSDatabase, although during a custom installation you have the option to change it. Setup creates and configures the database as needed.

- **Database Backups**

Setup creates a backup device for the database. It also schedules regular backups of the database. For more information, see [Job Schedule Worksheet](#) on page 35.)

Caution

Make sure that the schedules for database backup and Recovery Server jobs (such as Server Space Management and Integrity Check) do not coincide; otherwise data storage corruption can occur.

Security

Setup makes the following changes to Microsoft SQL Server security settings.

- **SQL Login**

To limit any security risks, Recovery Solution creates its own Microsoft SQL Server login (named **AeXRSDatabaseUser** by default) that it uses whenever it needs to access the Recovery Database. This login is a member only of the **db_owner** fixed database role (not the **sysadmin** role as it used to be Recovery Solution 6.1 and earlier versions) in and has full access only to the Recovery Database. Its default password is password.

Note

The default password cannot be changed.

- **Authentication**

If needed, the Recovery Server Setup changes the default authentication mode to SQL Server and Windows to allow authentication via the SQL login created specifically for Recovery Solution.

Note

For Recovery Solution to function properly, Notification Server admin must have dbo rights for Recovery Database.

Event Log Configuration

During server setup, Recovery Solution automatically makes the following changes to the configuration of the Windows event logs.

Event Log Table

Log	Change Made	Reason
System	Event Log Wrapping: Overwrite Events as needed.	Prevents warning messages from appearing on the server when the event log fills up.
Application	Maximum Log Size: 10240 KB (10 MB)	Ensures that enough log entries are retained so that troubleshooting can be performed if necessary.
Application	Event Log Wrapping: Overwrite Events as Needed	Prevents warning messages from appearing on the server when the event log fills up. Recovery Server uses this event log extensively, so it can fill up quickly.

We recommend that you leave these settings the way Setup has configured them.

Internet Information Server Configuration

This section describes the Microsoft Internet Information Server settings that Recovery Solution needs in order for the Web-based installation wizard to function properly. If you did not accept the default settings during IIS installation, or if you changed your IIS configuration, you might need to verify your settings with the list below.

The following virtual directories must exist in the IIS configuration on the server. Their settings must match those in the following table.

Virtual Directory Name	Agent	AsMext	LogFiles	WBFR
Actual Folder	The "AgentWeb" subfolder of the shared Recovery Agent installation subfolder of the program installation folder. By default, this is C:\Program Files\Altiris\Recovery Solution\Server\Agent\AgentWeb.	The "ASMext" subfolder of the shared Recovery Agent installation subfolder of the program installation folder. By default, this is C:\Program Files\Altiris\Recovery Solution\Server\Agent\ASMext.	The "LogFiles" subfolder of the "System32" subfolder of the Windows folder. By default, this is %WINDIR%\System32\LogFiles.	The folder where the Web-based file recovery program files are stored. If Web-based file recovery was configured automatically during installation of the server, then this is the folder that was specified for Web-based file recovery during Setup. By default, the folder is C:\Program Files\Altiris\Recovery Solution\Server\WBFR
Web access permissions	Read must be checked	None required.	Read must be checked.	Read must be checked.
Web application permissions	Execute (including scripts) must be selected.	Execute (including scripts) must be selected.	None required.	Script must be selected.
Default Document(s) for Web Browsing	Enable Default Document must be checked, and "Default.htm" must be included as a default document.	Not required.	Not required.	Enable Default Document must be checked, and "Default.asp" must be included as a default document.

Virtual Directory Name	Agent	AsMext	LogFiles	WBFR
Web Authentication Methods	<ul style="list-style-type: none"> • Basic Authentication must be checked. • Integrated Windows authentication (Windows 2000) 	<ul style="list-style-type: none"> • Allow Anonymous Access must be checked. • Integrated Windows authentication (Windows 2000) 	<ul style="list-style-type: none"> • Allow Anonymous Access must be checked. • Integrated Windows authentication (Windows 2000) 	<ul style="list-style-type: none"> • Integrated Windows authentication (Windows 2000)
Windows Folder Security Settings	<ul style="list-style-type: none"> • The SYSTEM user must have Full Access. • The AeXRS_Managers (or the name of your administrators group for Recovery Solution) must have Read access. • The AeXRS_Users (or the name of your administrators group for Recovery Solution) must have Read access. 	The Everyone user group must have Full Access.	The Everyone user group must have Full Access.	<ul style="list-style-type: none"> • For Windows 2000, the folder and all contents must have the Allow inheritable permissions from parent to propagate to this object box cleared. • The user group for Recovery Solution (by default AeXRS_Users) must have Read access to the main folder. • The Everyone user group must have Full Access to the following contents. <ul style="list-style-type: none"> All files in the "Image" subfolder. All files in the "Image" subfolder. All files in the "Image" subfolder. All "*.class" files. "FileDownload.asp" "GetFiles.asp" "GetFolders.asp" "Global.asa" "LogOff.asp" "ServerUtils.asp" "Styles.css"

Virtual Directory Name	AeXRSVault
Actual Folder	The "HTTPVault" subfolder of the shared Recovery Agent installation subfolder of the program installation folder. By default, this is C:\Program Files\Altiris\Recovery Solution\Server\HTTPVault.
Web access permissions	Read must be checked
Web application permissions	Execute (including scripts) must be selected.
Default Document(s) for Web Browsing	Enable Default Document must be checked, and "Default.htm" must be included as a default document.
Web Authentication Methods	<ul style="list-style-type: none"> • Basic Authentication must be checked. • Integrated Windows authentication (Windows 2000)
Windows Folder Security Settings	<ul style="list-style-type: none"> • The SYSTEM user must have Full Access. • The AeXRS_Managers (or the name of your administrators group for Recovery Solution) must have Read, List, and Execute access. • The AeXRS_Users (or the name of your administrators group for Recovery Solution) must have Read, List, and Execute access. • The XUSR_RepNDM user must have Read, List, and Execute access.

Notes

You can require users to establish an encrypted channel (https:// rather than http://) with your server before accessing the Web-based Setup Wizard or Web-Based File Recovery. The use of an encrypted channel, however, requires that the user's Web browser and your Web server both support the encryption scheme used to secure the channel. Before enabling encryption, you must install a valid server certificate. To require encryption in IIS, follow the procedure for enabling Secure Sockets Layer (SSL). For precise instructions, see the following topics in Internet Information Services section of Windows Help.

Enabling Encryption

Using Certificate Wizards

Obtaining and Installing Server Certificates

Configuring SSL

ODBC Configuration

During server setup, Recovery Solution configures Open Database Connectivity (ODBC) so that Recovery Solution can access its SQL Server databases. If you are having problems with Recovery Solution, you can verify that the configuration information is correct and update it yourself if necessary.

To set up the ODBC connection to the database

1. From the Windows **Start** menu, click **Settings > Control Panel**.
2. Open the ODBC applet.

The actual name of the applet varies depending on the version of Windows you are running. In Windows XP and Windows 2000, it can be found in the Control Panel **Administrative Tools** subfolder.

3. Click the **System DSN** tab.
4. Select **AeXRSDatabaseDSN** in the list and then click the **Configure** button.

If you do not see this entry, you can add it as follows.

- Click **Add**.
 - Click **SQL Server** from the list and then click **Finish**.
5. A wizard appears, walking you through the process of creating or modifying a data source to SQL Server. Set the values indicated below, and leave the defaults for any settings not mentioned here.
 - In the **Name** field, type **AeXRSDatabaseDSN**.
 - In the **Server** field, type the name of the server, then click **Next**.
 - Under **How should SQL Server verify the authenticity of the login ID?**, choose **With SQL Server authentication using a login ID and password entered by the user**.
 - Make sure the checkbox labeled **Connect to SQL Server to obtain default settings for the additional configuration options** is checked, then enter the SQL user name for Recovery Solution (the default name is **AeXRSDatabaseUser**) and its password, and click **Next**.
 - Click **Change the default database to**, then select the database for Recovery Solution (**AeXRSDatabase**) from the list.

Note

Check this box even if **AeXRSDatabase** already appears in the list.

- Click **Next**.
 - Click **Finish**.
 - A confirmation screen appears next. Click the **Test Data Source** button to verify that the ODBC connection is working properly.
You should then see a test results screen similar to the following.
6. Click **OK** in all open dialog boxes to complete the ODBC configuration.

DCOM Configuration

For secure communications among the server, consoles, and protected computers, Recovery Solution uses the Microsoft Distributed Component Object Model (DCOM), which consists of a set of system files installed on each computer. DCOM is a common operating system component that provides both flexibility and added security for many applications that run on a network.

Windows 2000/XP contains DCOM as part of the basic operating system. All Recovery Solution Setup programs configure DCOM as needed to run Recovery Solution.

Caution

In rare cases, the DCOM configuration might be changed so that Recovery Solution no longer works properly. This may happen when another, third-party, setup program has reinstalled or reconfigured DCOM improperly.

To set up DCOM on a protected computer

1. From the Windows **Start** menu, click **Run**.
2. Type `DCOMCNFG.EXE`, then click **OK**.
3. If the protected computer is running Windows XP, then do the following.
 - In the Console Tree, browse to **Console Root/Component Services/Computers/My Computer**, and select it in the list.
 - From the **Action** menu or the context menu, click **Properties**.
4. Click the **Default Properties** tab.
5. Make sure the following default values are set.
 - Enable Distributed COM on this computer is checked.
 - The Default Authentication Level setting is Connect.
 - The Default Impersonation Level setting is Impersonate.

This setting allows the server to use each protected computer's network account to perform actions on behalf of the protected computer. It prevents a protected computer from potentially using the network credentials of the server itself to perform operations that it would not be able to perform on its own.
6. Do one of the following.
 - **Windows 2000/XP Computers**
 - If the protected computer is running Windows XP, click **OK** to close the main DCOM properties dialog box, then in the Console Tree, expand **My Computer/DCOM Config**.
 - Scroll down the list until you see **Altiris Recovery Agent**, and select that item.

Do one of the following.

 - In Windows XP, from the **Action** menu or the context menu, click **Properties**.
 - In Windows 2000, click the **Properties** button.
 - Click the **Security** tab.

Click the option to specify custom access permissions, then click the **Edit** button. Make sure that following users appear in the list, and are allowed access.

 - **INTERACTIVE**

- **SYSTEM**

Note

If you prefer, you can choose to use default permissions and then make the security changes described below in the main DCOM properties. However, we strongly recommend that you use custom permissions for the objects, since you might not want all COM objects to have the rights you will assign to Recovery Solution.

- Configure the launch permissions to be the same as the access permissions you configured above.
- Click **OK** to close all open windows.

To set up DCOM on the server

1. From the Windows **Start** menu, click **Run**.
2. Type `DCOMCNFG.EXE`, then click **OK**.
3. Scroll down the list until you see Altiris Recovery Solution RemoteService, and select that item.

Recovery Solution Console uses this object to communicate with the server.

4. Click the **Properties** button, then click the **Security** tab.
5. Click **Use custom access permissions**, then click the **Edit** button. Make sure that following users and groups appear here.
 - The local AeXRS_Managers group (or the name of your administrator group for Recovery Solution)

- **INTERACTIVE**

- **SYSTEM**

Note

If you prefer, you can choose to use default permissions and then make the security changes described below on the main tabs of the Distributed COM Configuration Properties window. However, we strongly recommend that you use custom permissions for the objects, since you might not want all COM objects to have the rights you will assign to Recovery Solution.

6. Click **Use custom launch permissions**, then click the **Edit** button and add the same users as you added for the access permissions in the previous step.
7. Click **OK** until you get back to the main **Distributed COM Configuration Properties** window.
8. In the DCOM **Applications** list, scroll down until you see **Altiris Recovery Server**, and select that item.

Recovery Agent running on protected computers uses this object to communicate with the server.

9. Click the **Properties** button, then click the **Security** tab.
10. Click **Use custom access permissions**, then click the **Edit** button. Make sure that following users and groups appear here.

- **INTERACTIVE**

- **SYSTEM**

- The local AeXRS_Managers group (or the name of your administrator group for Recovery Solution)
- The local AeXRS_Users group (or the name of your user group for Recovery Solution)

Click **Use custom launch permissions**, then click the **Edit** button. Make sure that following users appear here.

- **INTERACTIVE**
- **SYSTEM**

Caution

Do *not* add **XUSR_RepNDM** or the AeXRS_Users local group to the **Launch Permissions** list. If you do, you will effectively lose control over when Recovery Solution is running. The reason is that this account is used automatically by all Recovery Agent installations. If it has launch permissions, then even if the service is stopped on the server, it will restart automatically as soon as a protected computer attempts to interact with the server.

11. Click **OK** until you get back to the main **Distributed COM Configuration Properties** window.
12. In the main **Distributed COM Configuration Properties** dialog box, click the **Default Properties** tab.
13. Make sure the following default values are set.
 - **Enable Distributed COM on this computer** is checked.
 - The **Default Authentication Level** setting is **Connect**.
 - The **Default Impersonation Level** setting is **Impersonate**.

This setting allows the server to use each protected computer's network account to perform actions on behalf of the protected computer. It prevents a protected computer from potentially using the network credentials of the server itself to perform operations that it would not be able to perform on its own.
14. Click **OK**.

Default DCOM security settings on the server

The following tables display the full default DCOM security settings which must be configured on the Recovery Server:

Abbreviations and acronyms

Launch and activation permissions:

LAct - Local Activation
 LL - Local Launch
 RAct - Remote Activation
 RL - Remote Launch

Access permissions:

LAcc - Local Access
 RAcc - Remote Access

def - default
 lim - limit

Default COM Security Permissions on the Recovery Server

Group or user names	LAct def	LL def	RAct def	RL def	LAct lim	LL lim	RAct lim	RL lim	LAcc def	RAcc def	LAcc lim	RAcc lim
INTERACTIVE	X	X	X	X								
SYSTEM	X	X	X	X					X			
Administrators	X	X	X	X	X	X	X	X				
IUSR_... (Internet Guest Account)					X	X	X	X				
IWAM_... (Launch IIS Process Account)					X	X	X	X				
Distributed COM Users					X	X	X	X			X	X
Everyone	X	X									X	X
SELF									X	X		
ANONYMOUS LOGON	X		X								X	X

AHMS {67B86D82-9B78-11D3-B597-00A0C91D0917}

Group or user names	LAct	LL	RAct	RL	LAcc	RAcc
INTERACTIVE	X	X	X	X	X	X
SYSTEM	X	X	X	X	X	X
AeXRS_Users	X	X			X	

Altiris Recovery Server (RSS) {864A9B22-6B68-11D1-9640-00C04FCD3EB0}

Group or user names	LAct	LL	RAct	RL	LAcc	RAcc
INTERACTIVE	X	X	X	X	X	X
SYSTEM	X	X	X	X	X	X
XUSR_RepNDM	X		X			

Group or user names	LAct	LL	RAct	RL	LAcc	RAcc
AeXRS_Users	X		X		X	X
AeXRS_Managers	X		X		X	X

**Altiris Recovery Solution RemoteService (RmtSvc)
{B438E666-9BE0-11D1-B83B-00A0C9843F26}**

Group or user names	LAct	LL	RAct	RL	LAcc	RAcc
INTERACTIVE	X	X	X	X	X	X
SYSTEM	X	X	X	X	X	X
XUSR_RepNDM	X	X	X	X	X	X

RPC Dynamic Port Allocation

DCOM uses Remote Procedure Call (RPC) dynamic port allocation to randomly select port numbers above 1024 by default. You can control which port range RPC dynamically allocates for incoming communication and then configure your firewall to confine incoming external communication to that port range, port 135 (the RPC Endpoint Mapper port) and ports 43189 - 43190.

To control RPC dynamic port allocation on the Recovery Server

1. From the Windows **Start** menu, click **Run**.
2. Type `DCOMCNFG.EXE`, then click **OK**.
3. In the Console Tree, browse to **Console Root/Component Services/Computers/My Computer**, and select it in the list.
4. From the **Action** menu or the context menu, click **Properties**.
5. On the **Default Protocols** tab, select **Connection-oriented TCP/IP** in the **DCOM Protocols** list and click **Properties** button.
6. In the **Properties for COM Internet Services** dialog box click **Add** button.
7. In the **Port range** text box add a port range (ex. 55000-55199), then click **OK**.
8. Leave the **Port range assignment** and the **Default dynamic port allocation** options set to **Internet range**.
9. Click **OK** to close all dialogs and restart the server computer.

On the client computer (optional)

1. From the Windows **Start** menu, click **Run**.
2. Type `DCOMCNFG.EXE`, then click **OK**.
3. In the Console Tree, browse to **Console Root/Component Services/Computers/My Computer**, and select it in the list.
4. From the **Action** menu or the context menu, click **Properties**.

5. On the **Default Protocols** tab move **Connection-oriented TCP/IP** to the top of the list.
6. Restart the computer.

Firewall Configuration

To use Recovery Server behind a firewall, a defined set of ports must be open to enable communication between the clients and the server. The following table lists these ports.

Protocol	Port	Direction
TCP and UDP	135 (DCOM)	Both
TCP	80 (HTTP)	Both
TCP	443 (HTTPS)	Both
TCP	43189	Inbound (to client)
UDP	43190	Inbound (to server)
TCP	>1024 (DCOM)	Both

When using DCOM for communication, you must open the port range (>1024) used for Remote Procedure Call (RPC) dynamic port allocation. For more information, see [RPC Dynamic Port Allocation](#) on page 30.

Notes

You must open port 80 in case you are using HTTP for communication between clients and Recovery Server.

You must open port 443 in case you are using HTTPS for communication between clients and Recovery Server.

You must open ports 135, 1024 and above in case you are using DCOM for communication between clients and Recovery Server.

You do not have to open port 43189 inbound to client if you enable the **Allow Recovery Agent to initiate scheduled snapshot** option in the Agent Settings.

By default, when the Recovery Agent service starts on protected computers running Windows XP or Windows 2003 Server, it will add port 43189 to the Windows Firewall Exceptions list. This functionality is controlled through the **Enable Altiris Recovery Agent to modify Windows Firewall settings** checkbox.

Web-Based File Recovery Configuration

Web-based file recovery is automatically configured during installation of the server, if all of the configuration requirements are met. If they are not, you can configure Web-based file recovery manually after the server is installed.

To configure Web-based file recovery manually

1. If the Web-based file recovery program files are not stored on a drive formatted with the Windows NT file system (NTFS), then do one of the following.
 - Move the WBFR folder to an NTFS drive on the server.

- Convert the drive where the Web-based file recovery program files are stored to an NTFS drive. You can do this using the Windows CONVERT.EXE command-line program.

Caution

Conversion to NTFS is an irreversible action. After converting a drive to NTFS, you cannot go back to the FAT file system without destroying the data on the drive.

2. On the server, open a command prompt and enter the following command.

```
REGSVR32.EXE "Web-based file recovery folder\WFEEngine.dll"
```

Replace Web-based file recovery folder with the full path to the Web-based file recovery program files (by default, this is C:\Program Files\Altiris\Notification Server\Client Recovery Server\WBFR), but a different folder might have been specified during installation of the server.

3. Open the Internet Service Manager program.

Note

In Windows 2000, the default **Start** menu shortcut is Start > Programs > Administrative Tools > Internet Services Manager.

4. Create a new virtual directory for the Web-based file recovery folder as follows.

- In the Console Tree, select the **Default Web Site** item for the server.
- From the **Action** menu or the context menu, click **New**, then click **Virtual Directory**.
- Step through the wizard until you are prompted to specify an alias for the virtual directory, then specify one.

The alias is the folder name that users will access when restoring files. To keep the configuration simple and consistent with the documentation, we recommend that you specify the default alias WBFR.

After you have specified an alias, click **Next**.

- Specify the full path to the folder containing the Web-based file recovery program files, then click **Next**.
- Accept the default access permissions, which should include **Read** and **Script** access, but nothing else.
Click the **Next** and Finish buttons as necessary to complete the wizard.

5. Configure the virtual directory as follows.

- In the Console Tree, select the virtual directory.
- From the **Action** menu or the context menu, click **Properties**.
Do one of the following.
- If the server is running Windows 2000, then on the **Virtual Directory** tab, change the **Application Protection** option to **Low (IIS Process)**.
- Click the **Documents** tab. Make sure that the checkbox labeled **Enable Default Document** is checked, and that **Default.asp** appears as one of the default file names in the list. If it does not, add it using the **Add** button.
Configure access to the virtual directory as follows.

- Click the **Directory Security** tab.
 - Under **Anonymous access and authentication control**, click the **Edit** button.
 - Clear the **Anonymous access** checkbox.
 - You may also clear the box labeled **Basic authentication (password is sent in clear text)**.
 - Check the box labeled **Integrated Windows authentication** (Windows 2000).
 - Click **OK** in all open dialog boxes until you return to the main Internet Service Manager window.
6. Configure Windows security for the Web-based file recovery program files as follows.

In the Web-based file recovery program files folder, open the properties for the following items, click the **Security** tab, and make sure that the **Everyone** group has **Full Access** rights to them.

All files in the "Image" subfolder.

The "Image" folder.

All "*.class" files.

"FileDownload.asp"

"GetFiles.asp"

"GetFolders.asp"

"Global.asa"

"LogOff.asp"

"ServerUtils.asp"

"Styles.css"

When you have finished, click **OK** to close the **Properties** dialog box.

- If the server is running Windows 2000, then for all files in both the main Web-based file recovery folder and the Images subfolder, click **Properties/Security** and clear the checkbox labeled **Allow inheritable permissions from parent to propagate to this object**, then click **OK**.
- Open the properties for the main Web-based file recovery program files folder, **WBFR**.
- Click the **Security** tab.
- If the server is running Windows 2000, clear the checkbox labeled **Allow inheritable permissions from parent to propagate to this object**.
- Give the user group for Recovery Solution (by default AeXRS_Users) the **Read** access permission to the folder.
- You can remove any other access rights to the folder, although you might want to give yourself and/or other administrators full access. (Even if you do not, you can add the permissions later if the need arises.)
- When you have finished configuring the security permissions, click **OK** to close the **Properties** dialog box.

Configuring Web-Based File Recovery to run on Windows Server 2003

1. On the Windows Server 2003 computer, open the Computer Management window by clicking Start > Programs > Administrative Tools > Computer Management.
2. Expand the **Services and Applications > Internet Information Services** item.
3. Right-click **Application Pool > New > Application Pool...**
4. Name the new application pool with a WBFR specific name. Example: "WBFR".
5. Click **OK**.
6. Right-click the new application pool and click **Properties**.
7. Click the **Identity** tab.
8. Select **Local System**.
9. Click **OK** and then click **Yes** on the warning shown.
10. Open properties of the **Default Web Site > WBFR**.
11. Under the WBFR Properties page, change the application pool for the WBFR virtual directory to the newly created application pool.
12. Click **OK** to save the changes.

Protected Computer IP Address Updates

Successful communications between the cluster and each protected computer require the use of the protected computer's IP address. The cluster keeps a record of each protected computer's IP address in the database.

In the event that a protected computer's IP address changes, the new information must be sent to the cluster to ensure that Recovery Solution continues working properly on that protected computer.

- If the IP address change requires the protected computer to be restarted, then the update does not occur until the computer is restarted.
- If the IP address change does not require the protected computer to be restarted, then the IP address update happens automatically the next time any of the following events occurs.
 - Approximately 5–10 minutes passes. Periodic updates are sent automatically.
 - Recovery Agent is restarted.
This normally occurs only when the computer is restarted, but it is also possible to restart Recovery Agent by stopping and starting the Control Panel service **Altiris Recovery Agent**.
 - A Dial-Up Networking connection on the protected computer is started or disconnected.
 - Snapshot on idle runs.

Job Schedule Worksheet

The purpose of this worksheet is to help you schedule various activities that need to run on the server. Since multiple activities running at the same time could slow down Recovery Solution, you might want to divide processing time among the various jobs to allow them to run more efficiently.

You can print this topic and fill in schedules as you create them. Some schedules are set by default when you install, but you can change them. The defaults are shown in the table below. The table also provides a sample schedule that you might wish to use as a guide.

Supplemental Table

Activity	Default Schedule	Actual Schedule	Sample
Manual Snapshots & Recoveries			Typically Occur Daily Monday - Friday 8:00 A.M. to 5:00 P.M.
Scheduled Snapshots	Daily Monday - Friday 7:00 A.M. to 7:00 P.M.		Daily Monday - Friday 7:00 A.M. to 7:00 P.M.
Server Space Management	Weekly Friday 6:00 P.M. to 11:59 P.M.		Daily Monday - Friday 5:00 A.M. to 7:00 A.M.
Report Table Updates	None		Daily 7:00 A.M. to 8:00 A.M.
Back Up the Server to Tape	None		Weekly Saturday 8:00 A.M.
Master Database Backup	Weekly Sunday 12:00 A.M. (Microsoft SQL Server default)		Weekly Sunday 12:00 A.M.
Database Backup	Weekly Sunday 5:00 P.M.		Weekly Sunday 5:00 P.M.

Supplemental Table (Continued)

Activity	Default Schedule	Actual Schedule	Sample
Deletion	None		Occasional Sunday after 5:00 P.M.
Integrity Check	Weekly Sunday 1:00 A.M. to 11:59 P.M.		Weekly Sunday 1:00 A.M. to 1:00 P.M.
Idle Time			Sunday after 5:00 P.M.

Chapter 3

Installing Recovery Solution

This chapter includes the following topics:

- [About Recovery Solution requirements](#) (page 37)
- [Setting up Recovery Solution prerequisite components](#) (page 37)
- [Installing the Recovery Solution product](#) (page 41)
- [Upgrading Recovery Solution](#) (page 42)
- [Licensing Recovery Solution](#) (page 44)
- [Uninstalling Recovery Solution](#) (page 45)

About Recovery Solution requirements

Recovery Solution requires the following:

- Symantec Management Platform 7.0 SP1

For more information on Symantec Management Platform prerequisites and installation instructions, see the *Symantec Management Platform Installation Guide*.

See <https://kb.altiris.com/article.asp?article=45732&p=1>

For client computer requirements, see "Recovery Agent Requirements" in the *Recovery Solution User's Guide*.

Setting up Recovery Solution prerequisite components

You may need to perform the following steps before you install Recovery Solution:

Step	Action	Description
Step 1	Install Symantec Management Platform 7.0 SP1	For more information on Symantec Management Platform prerequisites and installation instructions, see the <i>Symantec Management Platform Installation Guide</i> . See https://kb.altiris.com/article.asp?article=45732&p=1
Step 2	Discover manageable computers in your environment.	Discovery helps you find the hostnames of the computers where you can install the Altiris Agent to. See Discovering computers on page 40.

Step	Action	Description
Step 3	Install the Altiris Agent	The Altiris Agent lets the Notification Server get information from and interact with the client computers. See Installing the Recovery Solution product on page 41.
Step 4	(Optional) Install and configure a load balancer.	If you want to install and use more than one Recovery Server, you must use a load balanced cluster of servers. See Configuring the load balancer on page 38.
Step 5	Configure the SQL database.	For Recovery Solution to work correctly, you must set the SQL Server to mixed authentication mode. See Configuring the SQL Database on page 40.

Configuring the load balancer

If you are using more than one Recovery Server, you must use a load balanced cluster of servers. Install the load balancer according to the installation instructions of the manufacturer.

Recovery Solution supports the following load balancing technologies:

- Microsoft Network Load Balancing
See [About installing Microsoft Network Load Balancing](#) on page 38.
- BIG IP by F5 Networks, Inc.
See [About configuring the BIG IP Controller Health Monitors](#) on page 38

See [Setting up Recovery Solution prerequisite components](#) on page 37.

About installing Microsoft Network Load Balancing

Microsoft Network Load Balancing uses a virtual IP and MAC address. If the network hardware is not setup correctly, it can cause network collisions to occur. To prevent this we recommend the following:

- All Recovery Servers are connected to a network hub
- The network hub is connected to a programmable switch on your network
- Program the switched port address table with the Network Load Balancing virtual MAC address. Example: if your hub is plugged in to port 8 on your switch, program the switch that the Virtual MAC address is connected as port 8.

See [Configuring the load balancer](#) on page 38.

About configuring the BIG IP Controller Health Monitors

BIG IP health monitors verify connections and services on nodes that are members of load balancing pools. The monitor checks the node at a set interval. If the node does not

respond within a specified timeout period, the node is marked down and traffic is no longer directed to it. By default, an ICMP (Internet Control Message Protocol) monitor is associated with every node that is a member of a load balancing pool. This monitor is of the simplest type, checking only the node address and checking only for a ping response. To change the interval and timeout values of this default check, or to check specific services on a node, you need to configure a custom monitor or monitors to add to the default monitor.

For the default icmp monitor, we select the icmp monitor template, as shown below:

```
monitor type icmp {
  interval 5
  timeout 16
  dest *
}
```

The ICMP monitor template has three attributes: interval, timeout, and dest, each with a default value. (All monitor templates have these three basic attributes).

For the default monitor, template ICMP is used as is, that is, as monitor ICMP with its default attribute values. To change any of these default values, you would need to create a custom monitor based upon ICMP, for example, my_icmp. Only the values that are actually to be changed would need to be specified in the definition of the custom monitor. Therefore, if you wanted to change the timeout values only, you would define the custom monitor as follows:

```
b monitor my_icmp '{ use icmp timeout 20 }'
```

This would create a new monitor in /config/bigip.conf, as show below:

```
monitor my_icmp{
  #type icmp
  use "icmp"
  interval 5
  timeout 20
}
```

You can display this monitor using the following command:

```
b monitor my_icmp show
```

Once the custom monitor exists, you associate it with a node or nodes using the Configuration utility or the bigpipe node command. Example:

```
b node 11.11.11.1 11.11.11.2 11.11.11.3 monitor use my_icmp
```

Note

The nodes are identified by IP address only. ICMP can ping addresses only, not specific ports on addresses. This creates three instances of monitor my_icmp, one for each address. You can display the instances using the command **b node monitor my_icmp show**.

See [Configuring the load balancer](#) on page 38.

Configuring the SQL Database

If you plan to authenticate to the SQL Server using a Windows account, and if the SQL Server is set to Windows authentication mode only, you must set it to SQL Server and Windows (mixed) mode for Recovery Server to work correctly.

Caution

If you are using the Microsoft SQL 2005 Server, the `sys.xp_cmdshell` component is required before you can create a Recovery Cluster. To enable the component, go to **SQL Server 2005 Surface Area Configuration > Surface Area Configuration for Features > xp_cmdshell** and select the **Enable xp_cmdshell** checkbox. After the Recovery Cluster creation is complete, the component can be safely disabled.

See [Setting up Recovery Solution prerequisite components](#) on page 37.

To check or change the SQL authentication mode

1. Open the SQL Server Enterprise Manager (**Start > Programs > Microsoft SQL Server > Enterprise Manager**).
2. Right-click the SQL Server group you want to configure.
3. Click **Properties**.
4. Click the **Security** tab.
5. Under **Authentication**, select **SQL Server and Windows**.
6. Click **OK**.
7. Stop and restart the SQL service.

For more information, see your SQL Server documentation.

Discovering computers

Discovery lets you find the hostnames of the computers where you can install the Altiris Agent. You can discover computers on the network using a domain or a workgroup search.

For more information on Resource Discovery, see the *Symantec Management Platform Help*.

See [Setting up Recovery Solution prerequisite components](#) on page 37.

To discover computers

1. In the Dell Management Console, on the Actions menu, click **Discover > Import Domain Membership/WINS**.
2. In the Add Domain field, type the domain name and click the **Add** symbol.
3. Check **Domain Membership** and click **Discover Now**.
4. As the discovery process finishes, click **View discovery reports** to view the list of discovered computers.

Installing the Altiris Agent

The Altiris Agent is a program that you install on the computers you want to manage, allowing the Symantec Management Platform and solutions to get information from and

interact with your computers. The agent enables computers to receive configuration information from and send data to the Notification Server and helps download packages as well as tasks and jobs. The agent lets you change settings on the managed computer and install and manage various solution-specific plug-ins.

You must install the Altiris Agent on the computers you want to manage with Recovery Solution.

For more information on the Altiris Agent, see the *Symantec Management Platform Help*. See [Setting up Recovery Solution prerequisite components](#) on page 37.

To install the Altiris Agent

1. In the Dell Management Console, on the Actions menu, click **Agents/Plug-ins > Push Altiris Agent**.
2. On the Altiris Agent Installation page, install the Altiris Agent to computers in your environment.
For more information on how to install the Altiris Agent, see the *Symantec Management Platform Help* (Press **F1** or click **Help > Context** in the Dell Management Console).

Installing the Recovery Solution product

Use Symantec Installation Manager to install Recovery Solution.

You use Symantec Installation Manager to download and install Recovery Solution. You download and install Symantec Installation Manager and then use it to download and install the Symantec Management Platform and related products. You also use Symantec Installation Manager to repair, update, and apply licenses to Symantec Management Platform related products after you install them.

See <https://kb.altiris.com/article.asp?article=45732&p=1>

After installing Recovery Solution, you must perform the following tasks:

Task	Action
Task 1	Create a Recovery Cluster.
Task 2	Add Recovery Servers to the cluster.
Task 3	Configure the Recovery Cluster.
Task 4	Install the Recovery Agent on managed client computers.
Task 5	Verify the agent installation.

For instructions, see the 'Getting Started with Recovery Solution' chapter of the *Recovery Solution User's Guide*, or the *Recovery Solution Help*.

See [Where to get more information](#) (page 10)

After Server Installation Is Complete

After the Setup program for Recovery Server is complete, you should perform the following steps before continuing.

Check for Errors

The Recovery Server installation creates log files that record operations and errors that occurred during installation. The log files are text files that you can open in a text editor (such as Notepad). If any problems occurred, you should see them listed here. AeXCRSS.log lists all the high and medium level operations that server setup performed.

During installation, AeXCRSS.log is created in the temporary folder that is used for server installation (by default, C:\WINNT\Temp). After installation is complete, this file is copied to the folder where the Recovery Server is installed (by default, C:\Program Files\Altiris\Recovery Solution\Server).

You may want to open these files to verify that there are no error messages before continuing with your use of Recovery Solution.

Schedule Automatic Updates of Report Data

For more information, see "Using Recovery Solution Reports" in the *Recovery Solution User's Guide*.

Upgrading Recovery Solution

Before upgrading Recovery Solution we strongly recommend making a full offline backup of the Recovery Solution SQL Server database.

For more information, see [Recovery Solution Infrastructure Backup and Restore](#) on page 57.

Note

Upgrades from versions earlier than Recovery Solution 6.1 are not supported. For information on upgrading previous Recovery Solution installations to version 6.1 or later, see corresponding solution documentation.

To upgrade Recovery Solution perform the following steps:

Step	Action	Description
Step 1	Upgrade the solution.	Use Symantec Installation Manager to upgrade Recovery Solution. For more information on upgrading products, see the Symantec Installation Manager documentation.
Step 2	Upgrade Recovery Clusters.	See Upgrading Recovery Clusters on page 43.
Step 3	Upgrade Recovery Servers.	See Upgrading Recovery Servers on page 43.
Step 4	Upgrade Recovery Agents.	See Upgrading Recovery Agents on page 44.

For more information, see the *Recovery Solution Release Notes*.

See [Where to get more information](#) (page 10)

Upgrading Recovery Clusters

After you have upgraded the Recovery Solution program files, you must upgrade your Recovery clusters.

During the installation on Recovery Solution, a Recovery Cluster Upgrade policy is created. Use this policy to perform the upgrade process.

See [Upgrading Recovery Solution](#) on page 42.

To upgrade a cluster

1. In the Symantec Management Console, on the Home menu, click **Recovery Home**.
2. In the left pane, click **Configuration > Cluster Rollout > Cluster Rollout**.
3. On the Cluster Rollout page, click the cluster that you want to upgrade.
4. On the toolbar, click the **Upgrade Cluster** button.
5. (optional) In the Cluster Upgrade Progress dialog, check **Automatically start Recovery Server(s) upgrade after clusters upgrade completion**.

If you do not check this option, you can start the Recovery Server upgrade manually.

See [Upgrading Recovery Servers](#) on page 43.

6. Click **Run**.

The Cluster begins to upgrade. If the After Cluster upgrade, automatically start Recovery Server(s) upgrade checkbox was selected, the servers also upgrade; otherwise, you must, otherwise you must upgrade the servers manually. When the upgrade is completed you will need to restart the computer.

It will take a few minutes for the server component to install. To view the status of the server upgrade or to launch upgrade of the servers manually, see the Servers tab of the cluster properties page or the Recovery Server Upgrade policy on the Configuration tab of the Altiris Console (Configuration > Solution Settings > Incident Management > Recovery Clusters > Recovery Cluster Configuration).

Upgrading Recovery Servers

After Recovery Cluster upgrade, you must upgrade Recovery Servers. If you checked **Automatically start Recovery Server(s) upgrade after clusters upgrade completion** in the Cluster Upgrade Progress dialog, the Recovery Servers for this cluster will upgrade automatically.

You can also start the Recovery Servers upgrade manually.

Clicking the **Upgrade Server** button will only create and activate a Recovery Server software delivery policy that may arrive at the Recovery Server computer after a delay, dependent on the new configuration request interval that is set in the Targeted Agent Settings policy.

For more information, see the *Symantec Management Platform Help*.

If you wish to speed up the policy delivery process, on the Recovery Server computer, use the Altiris Agent to request the configuration (right-click on the Altiris Agent icon, click **Altiris Agent Settings** and then click **Update**).

Note

If the server upgrade failed, you can restart the upgrade by logging in to the Recovery Server computer and executing Setup.exe from \\<NS Server>\NSCAP\Bin\Win32\X86\Recovery Server Package location.

See [Upgrading Recovery Solution](#) on page 42.

To upgrade a Recovery Server

1. In the Symantec Management Console, on the Home menu, click **Recovery Home**.
2. In the left pane, click **Configuration > Cluster Configuration > Server Rollout**.
3. On the Server Rollout page, click the server that you want to upgrade.
4. On the toolbar, click the **Upgrade Server** button.

Upgrading Recovery Agents

After you upgraded Recovery Clusters and Recovery Servers, upgrade the Recovery Agents that are installed on the client computers.

Upgrading Recovery Agents may take some time, dependent on the new configuration request interval that is set in the Targeted Agent Settings policy.

For more information, see the *Symantec Management Platform Help*.

See [Upgrading Recovery Solution](#) on page 42.

To upgrade Recovery Agents

1. In the Symantec Management Console, on the Home menu, click **Recovery Home**.
2. In the left pane, click **Configuration > Agent Rollout > Recovery Agent Upgrade**.
3. Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
4. Click **Save changes**.

Licensing Recovery Solution

Each Altiris product comes with a 7-day trial license that is installed by default. You can register and obtain a 30-day evaluation license through our Web site at www.altiris.com or purchase a full product license.

Use Symantec Installation Manager to license Recovery Solution.

For more information on licensing, see the Symantec Installation Manager documentation.

Uninstalling Recovery Solution

To uninstall Recovery Solution perform the following steps:

Step	Action	Description
Step 1	Uninstall the Recovery Agents.	See Uninstalling the Recovery Agents on page 45.
Step 2	Uninstall Recovery Servers.	See Uninstalling Recovery Servers on page 45.
Step 3	Uninstall Recovery Clusters.	See Uninstalling Recovery Clusters on page 46.
Step 4	Uninstall Recovery Solution.	Use Symantec Installation Manager to uninstall Recovery Solution. For more information on upgrading products, see the Symantec Installation Manager documentation.

Uninstalling the Recovery Agents

Uninstalling Recovery Agents from the client computers may take some time, dependent on the new configuration request interval that is set in the Targeted Agent Settings policy.

For more information, see the *Symantec Management Platform Help*.

See [Uninstalling Recovery Solution](#) on page 45.

To uninstall Recovery Agents

1. In the Symantec Management Console, on the Home menu, click **Recovery Home**.
2. In the left pane, click **Configuration > Agent Rollout > Recovery Agent Uninstall**.
3. Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
4. Click **Save changes**.

Uninstalling Recovery Servers

After you uninstalled Recovery Agents, uninstall Recovery Servers.

Uninstalling Recovery Servers may take some time, dependent on the new configuration request interval that is set in the Targeted Agent Settings policy.

For more information, see the *Symantec Management Platform Help*.

See [Uninstalling Recovery Solution](#) on page 45.

To uninstall a Recovery Server

1. In the Symantec Management Console, on the Home menu, click **Recovery Home**.
2. In the left pane, click **Configuration > Cluster Configuration > Server Rollout**.
3. On the Server Rollout page, click the server that you want to uninstall.

4. On the toolbar, click the **Uninstall Server** button.

Uninstalling Recovery Clusters

Uninstalling the cluster uninstalls all Recovery Servers that assigned to this cluster, the database is deleted, and then the cluster is deleted from the CMDB.

This action does not remove the BLOB files in the storage. You must manually delete the files after deleting the storage.

See [Uninstalling Recovery Solution](#) on page 45.

To uninstall a cluster

1. In the Symantec Management Console, on the Home menu, click **Recovery Home**.
2. In the left pane, click **Configuration > Cluster Rollout > Cluster Rollout**.
3. On the Cluster Rollout page, click the cluster that you want to uninstall.
4. On the toolbar, click the **Uninstall Cluster** button.

Chapter 4

Command Line Utilities

This chapter contains information about the following utilities:

- [AeXRSEnc Utility](#) (page 47)
- [AeXMigrt.com Utility](#) (page 50)

AeXRSEnc Utility

AeXRSEnc.exe utility lets administrator encrypt and decrypt the *policy.cfg* file that contains Recovery Agent settings on client computers. The utility is especially useful in case Recovery Solution is installed without Notification Server. In this case administrator can modify Recovery Agent setup package to contain custom agent settings.

The *recovery.xml* file is an ASCII file that controls where the Recovery Agent stores its settings and accessibility to which tabs in the agent UI is controlled via password. This file is encrypted using Microsoft's implementation of RC2 algorithm with 40bit encryption key. This algorithm is widely used in a number of commercial software packages, including Lotus Notes, Microsoft Windows, Internet Explorer and Netscape Communication's Navigator and Communicator (refer to the RSA Data Security, Inc. web site at <http://www.rsasecurity.com> for more details on this algorithm).

To replace the *policy.cfg* file in AgentSetup.exe package you can use the ASPack utility found in *install path\Altiris\Recovery Solution\Console\Tools* folder on the computer where Recovery Solution is installed.

To download the AeXRSEnc utility

1. In the Altiris Console, click the **Tasks** tab.
2. In the left pane, select **Tasks > Incident Resolution > Recovery Solution > Agent Settings Decryption/Encryption Utility**.

AeXRSEnc utility usage

To encrypt the *recovery.xml* file outputting the encrypted *recovery.cfg* file in the current working directory, run:

```
AeXRSEnc.exe -e|-encrypt
```

To decrypt the *recovery.cfg* outputting the decrypted *recovery.xml* file in the current working directory, run:

```
AeXRSEnc.exe -d|-decrypt
```

For help, run:

```
AeXRSEnc.exe -h|-help
```

Policy XML File Description

The client settings stored in .XML files (*policy.cfg* and *usrcfg.xml*) are installed with Recovery Agent. These .XML files can be found in the Recovery Agent's Config folder. The *policy.cfg* file is encrypted and contains all Recovery Agent settings; the *usrcfg.xml*

is stored in plain text and contains custom user settings (the file is empty by default). To encrypt or decrypt the policy.cfg file you must use the AeXRSEnc.exe utility.

The policy.cfg reflects the settings from the Altiris Console; the non-encrypted usrcfg.xml contains custom user settings, which will override the settings defined in Console in case the permissions are set to allow it. The usrcfg.xml has the same XML structure that the policy.cfg has, except the **inherit** and **permission** attributes and some other sub-categories, which can not be modified through the Recovery Agent Options, such as **<UserRight>**, **<HealthAlerts>**, **<SpaceUsage>** etc. The policy.cfg must contain all the settings (none of them can be deleted from policy.cfg), but the usrcfg.xml file can be empty.

All Recovery Solution settings are grouped together under different categories. On the top level, all Recovery Agent settings are divided into three categories that reside inside the **<AgentSettings>** root XML tag:

```
<AgentSettings>
  <RemoteSettings>
    ...
  </RemoteSettings>

  <CommonSettings>
    ...
  </CommonSettings>
</AgentSettings>
```

The **<RemoteSettings>** category contains Recovery Agent settings. The **<CommonSettings>** category contains common settings the Recovery Agent.

Inside the top three categories, the settings are grouped by sub-categories, such as:

- **<SnapshotSettings>** - Snapshot and Snapshot Schedule settings
- **<SnapshotExcludes>** - Snapshot excludes
- **<RollbackExcludes>** - Rollback excludes
- **<SpaceManagement>** - Space Management settings
- **<SpaceUsage>** - Storage quota settings
- **<HealthAlerts>** - Health Alerts settings
- **<BandwidthThrottling>** - Bandwidth Throttling settings
- **<MiscSettings>** - Miscellaneous settings
- **<ConnectionManagement>** - Connection Management settings
- **<UserRights>** - User rights
- **<RemoteAccessSettings>** - Remote Access settings
- **<TransportSettings>** - Transport settings
- **<HiddenTransportSettings>** - Transport settings that depend on cluster network settings
- **<StorageManagement>** - Storage settings

The sub-categories contain two attributes (that exist only in policy.cfg file and absent in usrcfg.xml): **permission** and **inherit**. The **permission** attribute controls the settings behavior. The **inherit** attribute is not used by Recovery Agent, it was reserved for the Altiris Console usage only. The **permission** attribute can have one of the three values:

- **ReadOnly** - the settings for this sub-category are taken from policy.cfg and cannot be modified by user from the Recovery Agent Options.
- **Edit** - the settings for this sub-category could be overridden by user settings modified from the Recovery Agent Options. The overridden settings are stored in usrcfg.xml. In case of **Edit** permission, the settings for current sub-category will be first looked up in usrcfg.xml and if they are absent then the settings will be taken from policy.cfg.
- **Append** - this attribute is used only for Snapshot and Rollback excludes. In case of the **Append** permission, the settings (list of excludes) are taken from policy.cfg and usrcfg.xml.

Caution

We do not recommend manual modification of policy.cfg or usrcfg.xml files, because any misprint can cause the Recovery Agent to become totally unusable. The best practice is to modify the settings from the Altiris Console.

Here is the example of how to modify the **Hide client UI** settings using the policy file:

- Get the AeXRSEnc.exe utility and copy it to the Recovery Agent Config subfolder. Then run it using the following command line:

```
AeXRSEnc.exe -d
```

This will decrypt the policy.cfg file to policy.xml.
- Find the **HideClientUI** tag that reflects the **Hide client UI** settings in the Altiris Console and modify this setting (set to **enabled** attribute to **True**)
- Check that XML file format is correct and readable by opening it using the Microsoft Internet Explorer.
- If XML file is correct, then delete policy.cfg file and run the following command line to encrypt policy.xml file to policy.cfg:

```
AeXRSEnc.exe -e
```
- To force the Recovery Agent rereading policy.cfg file and to apply the modified setting, run the following command in the Recovery Agent folder:

```
AeXCmd.exe /ApplySettings
```

Here is the example how to modify the scheduled snapshot starts time:

- Decrypt the policy.cfg file using the AeXRSEnc.exe utility (like in previous example).
- Locate the **<StartTime>** tag inside the **<SnapshotSettings>** sub-category in policy.xml file.
- Modify the time inside the **<StartTime>** tag (please use the same time format).
- Check the policy.xml file and encrypt and apply it like in the previous example.

The following figure shows sample policy.xml file settings. Note that to hide all Recovery Agent user interface elements, the **enabled** attribute of the **<HideClientUI>** tag must be **True**, and the following **<CommonSettings>** must be **False**:

- **<ShowStatusIcon>**

- <ShowAgentDesktopIcon>
- <ShowAgentDesktopIcon>
- <ShowAgentOptionsInStartMenu>
- <ShowWelcomeScreen>

AeXMigrt.com Utility

The purpose of the AeXMigrt.com utility installed with Recovery Solution into the folder *install path*\Altiris\Recovery Solution\Console\Tools on Notification Server computer is to let administrators automate retrieval of files from the Recovery Server for a client or a set of clients.

This section contains the following topics:

- [Overview](#) (page 50)
- [Command-line parameters](#) (page 52) (with usage examples)
- [Input XML files](#) (page 54) (with usage examples)

Overview

The AeXMigrt.com utility runs on a computer where Recovery Agent installed and configured to connect to the Recovery Server to restore files from. Utility accesses the Recovery Server using the Recovery Agent, so the Recovery Agent must be fully functional (not disabled) on the computer.

Note

We recommend disabling scheduled snapshots and snapshots on events for the client, otherwise these snapshots can affect the utility workflow.

The utility can run on Microsoft Windows 2000 and later platforms.

The utility uses command-line parameters , the list of protected computers and the search mask supplied at run time to perform the following operations:

- Authenticate on the Recovery Server to obtain the list of files for specified protected computers.
- Create a list of files that must be restored.
- Initiate restore operation using the Recovery Agent.

Note

The utility is command-line based and exposes no UI.

Use cases

Administrator wants to locate and restore a particular file (including all revisions) from selected computers backing up to the Recovery Server. The utility automatically creates folders for each computer where the file exists during the restore. When multiple revisions of the file exist then the incremental ID is added to the name of the file revision (myfile001.txt, myfile002.txt etc.). The destination folder can be a local drive or a network share.

Restore

The utility lets the user restore files or folders by their name, name mask or location. Also, it is possible to restore files from a particular date range. There is no UI available for the search pattern configuration — all options must be provided using the command-line parameters or in an XML file.

To search for files, the utility enumerates files that were backed up from a particular client to the Recovery Server and applies the specified mask to locate the required files. The search engine creates the list of files that fall under specific criteria specified by the user and will be restored.

Note

Specifying a more precise search mask will significantly decrease the search time.

The utility performs an automated restore for files specified by the supplied mask and that were backed up from the specified computers to the Recovery Server. The utility accepts the file or folder name masks and the list of computers as input parameters, searches for these files on the Recovery Server and submits the restore job for the found items. The utility waits for the submitted job to complete and logs the resulting event into the activity log.

The restore itself is performed by the Recovery Agent, using the list of found files. The utility creates the restore specification and submits the restore jobs to the Recovery Server. Depending on the number of files found, the utility submits either one or more restore jobs. In case of multiple jobs, utility submits them one by one, waiting for each job to complete.

Destination folder for a restore operation must be provided using the command-line or the default one will be used. The default subfolder "aex_restored" is created in the location from where the utility has been launched.

Restored file naming

If you restore only latest revisions, the files will have exactly the same name they were backed up under on the Recovery Server. If you restore all revisions, the restored files that have multiple revisions will be renamed using following pattern:

original_file_name(revision_number).original_extension

So if the file "mymail.pst" has 10 revisions and "restore all revisions" parameter was specified, the restored folder will contain files:

Mymail(001).pst

Mymail(002).pst

...

Mymail(010).pst

All file creation and modification dates will be restored correctly for corresponding versions, and it is up to the user to find the required one.

Authentication

The utility accesses the Recovery Server under a logged-on user account or an account specified in the command-line parameters or the specified XML file. If the utility fails to access the Recovery Server using the specified credentials, it will log the corresponding entry into the log file.

The utility accepts accounts from the AexRSUsers or AeXRSMangers groups. For an account from the AexRSUsers group, only files from protected computers that belong to the particular user can be restored. For accounts from the AeXRSMangers group, the files from all protected computers can be restored.

Destination folder structure

The restored files will be placed in the destination folder as follows: <destination folder>\<computer name>\<disk name>\<path to file>. So, if the destination folder is C:\Tmp and original file is D:\Program Files\PST\mypst.pst on machine XRG200 then the resulting restored file path will be:

C:\Tmp\XRG200\D\Program Files\PST\mypst.pst

Activity and error logging

During execution, the utility creates the activity log file that contains the description and details of performed operations. The default log file name is "ade.log" and it will be created in the same folder where utility resides by default. The log file path can be changed by providing the special command-line parameter.

The log file will contain following information:

- Utility executions start time
- Name of the currently logged user
- Name of the Recovery user selected to authenticate on Recovery server
- List of machines that are available for search
- Destination folder
- List of found files
- Any information about errors that occur during execution

Any internal utility errors that occur the execution will be logged to the activity log file. Any errors that occur during the restore job execution and the status of restore operation for found files will be logged into the Windows application log as usual.

Command-line parameters

The restore operation can be started by specifying the mandatory "/R" parameter. All other parameters are optional. The following table lists the parameters recognized the by utility.

Parameter	Description
/R	Performs restore
/M:<computer_name>	Specifies the particular client machine name or name mask to search files for. If not specified, utility will search files on all machines that can be accessed by user specified in logon dialog.
/File:"<file_name>"	Specifies the file name or file name mask to search for. More than one mask can be specified. Optional, if no masks (file or folder) specified, all files will be restored.

Parameter	Description
<code>/Folder:"<folder_name>"</code>	Specifies the folder or folder mask to search for. More than one mask can be specified. Optional, if no masks (file or folder) specified, all files will be restored.
<code>/All</code>	Specifies that all revisions of found file must be restored. Optional, if not specified latest revisions of file(s) will be restored. Valid only for restore operation.
<code>/FromDate:"MM/DD/YY"</code>	Specifies an optional time based filter. Only file revisions that are newer than specified date will be restored. The utility will accept only one mask of this type but it can be used with <code>/ToDate</code> . Valid only for restore operation.
<code>/ToDate:"MM/DD/YY"</code>	Specifies an optional time based filter. Only file revisions that are older than specified date will be restored. The utility will accept only one mask of this type but it can be used with <code>/FromDate</code> . Valid only for restore operation.
<code>/XML:<full_path_to_xml></code>	Specifies a full path to XML file with parameters for restore/deletion operation. If specified, the utility will obtain search masks and other parameters from XML file. NB! Parameters provided from command line will override parameters from XML file, except search masks and client machines that will be used as additional to one specified in XML. See Input XML files (page 54).
<code>/Dest:<destination_folder></code>	Valid for restore operation, specifies a folder to restore found files into. Optional, if not specified, utility will restore found files into its current location subfolder <i>aex_restored</i> . The destination can be local, UNC path, or a mapped network location.
<code>/S</code>	Stops execution of previously started restore operation.
<code>/Login</code>	Login name (DOMAIN\User) to authenticate on Recovery Server. Optional, if not specified, utility will try to authorize under currently logged user.

Parameter	Description
/Pass	Password to authenticate on Recovery Server. Optional, if not specified (but /Login was specified), empty password will be used. Ignored if "/Login" was not specified.
/L:<log_file_path>	Full path to log file that will be generated by utility. Optional, if not specified, utility will generate log file in folder where it resides.
/?	Displays a dialog with utility usage scenarios.

Usage examples

The following table gives some examples on how the restore operation can be configured from the command line.

Sample task	Command
Search all clients and restore all found PST files	AexMigrt.com /R /File:"*.pst"
Search all clients and restore all found Word and Excel documents	AexMigrt.com /R /File:"*.doc" / File:"*.xls"
Search client XRG200 for folder C:\Documents and restore its content.	AexMigrt.com /R / Folder:"C:\Documents" / M"XRG200"
Search all clients and restore all found PST files into c:\tmp folder using ALTIRIS\Britney account with password "oops".	AexMigrt.com /R /File:"*.pst" / Login:"ALTIRIS\Britney" / Pass:oops /Dest:"C:\tmp"
Search all clients and restore all revisions of found PST files that were included in snapshots performed between 10/11/2006 and 10/12/2006.	AexMigrt.com /R /File:"*.pst" / All /FromDate:"10/11/2006" / ToDate:"10/12/2006"
Cancel restore.	AexMigrt.com /S

Input XML files

The most convenient way to perform a restore is using an XML file passed to the utility through the command line. While the XML file can contain all parameters required to perform the restore, these parameters can be overridden or extended by using the corresponding command-line parameters.

Note

File masks provided in an XML file should not contain reserved symbols for XML syntax. For example, you cannot use symbols "<", ">", "(", ")" and other. If you need to use a file or folder mask with these symbols, use the command-line parameters instead of XML file.

Sample XML file 1

The following sample XML file (adeu.xml provided with the utility) configures the utility to restore latest revisions of two files and all folders on disk C: that start with "Photo" on computers PC1, PC2, PC3. The Recovery Server will be accessed under "ALTIRIS\Britney" user account with password "oops". All activity logging will be performed into "C:\britney.log" file.

```
<?xml version="1.0" encoding="utf-8"?>
<Operations>
  <Operation type="restore" Dest="c:\Tmp" Login="ALTIRIS\Britney"
  Pass="oops" LogFile="C:\britney.log" FromDate="10/11/2006"
  ToDate="20/11/2006">
    <Machines>
      <Machine Name="PC1"/>
      <Machine Name="PC2"/>
      <Machine Name="PC3"/>
    </Machines>
    <SearchItems>
      <Item type="File" Name="party.img"/>
      <Item type="File" Name="mail.pst"/>
      <Item type="Folder" Name="C:\photo*"/>
    </SearchItems>
  </Operation>
</Operations>
```

Sample XML file 2

The following sample XML file configures the utility to restore all revisions of two files "party.img" and "mail.pst" and all revisions of files in all folders on disk C: that starts with "Photo" that were modified between 10/11/2006 and 10/12/2006. This operation will be performed for all computers to which currently logged user has access. The Recovery Server will be accessed under currently logged-on user account. All activity logging will be performed into "C:\britney.log" file.

```
<?xml version="1.0" encoding="utf-8"?>
<Operations>
  <Operation type="restore" Dest="c:\Tmp" LogFile="C:\britney.log"
  Versions="all" FromDate="10/11/2006" ToDate="10/12/2006">
    <Machines>
    </Machines>
    <SearchItems>
      <Item type="File" Name="party.img"/>
    </SearchItems>
  </Operation>
</Operations>
```

```
<Item type="File" Name="mail.pst"/>
  <Item type="Folder" Name="C:\photo*" />
</SearchItems>
</Operation>
</Operations>
```

Overriding XML values with command-line parameters

It is possible to override parameters specified in XML file by providing corresponding parameters from command line:

The following sentence executes the restore operation for the XML file specified above using "D:\restoredstuff" folder as destination.

```
AexMigrt.com /XML:"adeu.xml" /Dest:"D:\restoredstuff"
```

The following sentence executes the restore operation for XML file specified above using "D:\restoredstuff" folder as destination and adds one more computer to search for in - PhotoVault:

```
AexMigrt.com /XML:"adeu.xml" /Dest:"D:\restoredstuff" /
M:PhotoVault
```

Chapter 5

Recovery Solution Infrastructure Backup and Restore

This chapter describes the steps that need to be done in order to obtain a complete backup of Recovery Solution infrastructure.

- [Recovery Solution Infrastructure](#) (page 57)
- [Backup](#) (page 57)
- [Restore](#) (page 61)

Recovery Solution Infrastructure

A Recovery Cluster may have one or several Recovery Servers, which can be installed remotely. A cluster's Recovery Database can be also located on a remote SQL server.

One Notification Server can manage many Recovery Clusters.

The Notification Server Database stores the following Recovery Solution data: list of Recovery Clusters, Recovery Agent and Recovery Cluster settings.

Through Recovery Solution data file mirroring, there can be several copies of data files, these copies are synchronized between themselves either synchronously or asynchronously (by means of an Recovery Server job).

You can have an optional load balancer device that can be "attached" to the cluster. It is used to distribute client requests among the cluster's servers.

As a result, the Recovery Solution infrastructure can be now heavily distributed:

- The SQL Server computer with Notification Server Database.
- A Windows Server computer with Notification Server and Recovery Solution.
- Each Recovery Cluster can have its own SQL Server computer with Recovery Database.
- Any number of Recovery Server computers. Every such computer has its own local Windows group for Recovery Solution users; it also has ODBC DSN string for communication with the Recovery Database computer.

Backup

Generally, to get a complete snapshot of an Recovery Solution installation, you must back up the following pieces of information:

- On computer with SQL Server that hosts the Notification Server Database:
 - The Notification Server Database. Either the complete database must be backed up, or only Recovery Solution-related data (see [Notification Server Database Backup](#) on page 58).
 - "Linked Server" entries to SQL Server computers with Recovery Database. SQL Server Enterprise Manager allows doing this easily via right-click on "Linked

Servers" node in the Enterprise Manager console, and selecting "Export List..." menu item.

Note

This step is only needed if the Notification Server database is located on a different SQL server rather than Recovery database.

- On computers with SQL Servers that host Recovery Database (for all Recovery Clusters):
 - The Recovery Database (see [Recovery Database Backup](#) on page 59).
 - AeXRSDatabaseUser login account
This account can be seen under Security\Logins node in the Enterprise Manager console. Right click provides "Export List..." menu item.
- For every Recovery Cluster, Recovery Solution data files must be backed up as well (see [Data Files Backup](#) on page 60).
- For clusters that use load balancers, load balancer configuration must be backed up. Since this information is balancer-dependent, there is no step-by-step instruction for backup procedure. Please refer to the specific load balancer's documentation.

Notification Server Database Backup

If Notification Server is only used to host the Recovery Solution installation, you can back up the complete Notification Server Database. The Notification Server Database can be backed up using approaches described in [Recovery Database Backup](#) on page 59 except that you will specify the Notification Server Database.

Note that if the SQL Backup Agent is not used, then the SQL Server service that hosts the Notification Server Database must be stopped, which will make the Notification Server non-operable for the duration of Notification Server Database backup.

But if there are several solutions installed, it's not feasible to back up the complete Notification Server Database, as in case of disaster the whole database will have to be restored, possibly overriding other solution's settings. For this scenario, a set of SQL scripts was developed. These scripts are available for download.

- Backup_All_RS_Clusters.sql - creates a backup database named RS_Backup_DB, then backs up all RS clusters-related data into that database.
http://www.solutionsam.com/imports/7_0/recovery/backup_all_rs_clusters.sql
- Restore_All_RS_Clusters.sql - restores information about all RS clusters from the RS_Backup_DB.
http://www.solutionsam.com/imports/7_0/recovery/restore_all_rs_clusters.sql
- Backup_Single_RS_Cluster.sql - backs up information about a single cluster.
http://www.solutionsam.com/imports/7_0/recovery/backup_single_rs_cluster.sql
- Restore_Single_RS_Cluster.sql - restores information about a single cluster.
http://www.solutionsam.com/imports/7_0/recovery/restore_single_rs_cluster.sql
- Create_RS_Backup_DB.sql - creates an empty RS_Backup_DB. Should be called before Backup_Single_RS_Cluster.sql in cases when there is no backup database.
http://www.solutionsam.com/imports/7_0/recovery/create_rs_backup_db.sql

Caution

These scripts do not backup RS Agent Settings and RS Agent Rollout policies. So changes to these settings will be lost after restore.

Notes

Every script has a comment in the beginning, describing its usage.

Before running Backup_Single_RS_Cluster.sql and Restore_Single_RS_Cluster.sql scripts, you must specify proper cluster GUID. To get the Recovery Cluster GUID, open Properties for the Recovery Cluster you want to back up in the Altiris Console.

Recovery Database Backup

For every Recovery Cluster, its Recovery Database must be backed up.

It is strongly recommended that you back up the database to removable storage on a regular basis. For that, you can use the SQL Server database backup functionality built-in the Microsoft SQL Server software.

Important

Whichever method you use, back up the database files first and then the protected data (BLOB) files. Also, because Recovery Solution uses the domain user accounts database, the domain controller computer must be also backed up.

The following instructions help you backup the Recovery Database. For additional information on backup and restore of Microsoft SQL Server databases, see Microsoft SQL Server documentation.

To backup the database

1. Stop the Recovery Server service.

See "Stopping and Starting the Recovery Server Service" in the *Recovery Solution User's Guide*.

2. If the server is running Microsoft SQL Server:
 - a. Open SQL Enterprise Manager.

Note

For Microsoft SQL 2005, Microsoft SQL Server Management Studio should be used.

- b. In the Console Tree (usually on the left side), expand **SQL Server Group**, the name of the server, and then **Databases**.
- c. Select the database for Recovery Solution.
By default, it is named AeXRSDatabase.
- d. In the Details Pane, under Backup, click **backup database**.
- e. Under Backup, click **Database - complete**.
- f. Under Destination, click **Add**.
- g. In the Click Backup Destination dialog box, click **File name**.
- h. Specify the full path and file name. You can use the ... button to locate a path.

The path is where the database backup will go. The file name is the file that you will have your backup software back up.

- i. Click **OK**.
 - j. Click **Overwrite existing media**.
 - k. Click **OK to start the backup**.
 - l. Have your backup software back up the file you created.
3. If the server is running MSDE:
- a. Open an MS-DOS style command prompt.
 - b. Change to the BINN subfolder of the folder containing the MSDE program files. You can use a command such as the following.

```
CD /D "D:\MSSQL7\BINN"
```
 - c. Enter the following command.

```
OSQL.EXE -U sa -P -n -Q "BACKUP DATABASE AeXCRDatabase TO DISK = 'e:\AeXCRDatabase.dat'"
```

AeXRSDatabase is the default name of the database. If your installation of Recovery Solution uses a different database name, make the appropriate changes in the above command. The path and file name specified at the end can be modified to any appropriate location.

This command could be scheduled through Windows Task Scheduler or the AT command-line program. Database backups can also be scheduled using a SQL script. For details, see the Microsoft knowledge base article Q241397, which is available on the Microsoft Web site (<http://www.microsoft.com>).
4. Use your backup software to back up the protected data (BLOB) files. See [Data Files Backup](#) (page 60).

Data Files Backup

For every Recovery Cluster, its data files must be backed up. After the synchronization job is complete, only one copy of the data files (from any group) should be backed up. All servers in the clusters must be stopped or disabled during this process, to ensure data integrity.

Backing Up With Software That Includes a SQL Backup Agent

Follow these steps if your backup software includes a SQL backup agent. You might also need to refer to the instructions for your backup software.

1. Back up the database files for Recovery Solution.
By default, these are the following.
 - The main data file is AeXRSDatabase_Data.MDF, in a folder named AeXRSDatabase.
 - You might have additional data files. Typically the next name would be AeXRSDatabase_Data.NDF.
 - The log file is AeXRSDatabase_Log.LDF, in a folder named AeXRLog.
2. Back up the protected data (BLOB) files.

Load Balancer Configuration Backup and Restore

Note

This step is only needed if your Recovery Cluster is uses load balancer.

Since in Recovery Solution 7.0 the load balancer device configuration (such as adding the nodes) must be performed manually, backup and restore must also be performed manually. What exactly should be backed up and restored is balancer-dependent, generally information about nodes and about protocols/ports should be preserved and restored.

Note that any changes to the restored configuration, such as balancer address, must be reflected in the Recovery Cluster settings UI in the Altiris Console.

Restore

If only the Recovery Database or the data files got corrupted, there is no need to restore the Notification Server Database. In such cases skip the "Notification Server Database Restore" section.

Similarly, if only the Notification Server Database got corrupted, there is no need to restore the Recovery Database or data files of Recovery Clusters.

Note, however, that if the Notification Server Database is restored from an old backup, then the restored database will not contain information about recently created Recovery Clusters and their settings.

The Recovery Solution can be restored using either of the two approaches:

If whole Notification Server database is restored

In this case Notification Server and Recovery Database should be simply restored using SQL server tools (see [Notification Server Database Restore](#) on page 62), data files should be restored to original location and Recovery Server should be installed if original installation was corrupted. If Recovery Database was created on different SQL server than Notification Server database, then saved ODBC DSN string should be restored as well.

If only Recovery Solution specific information is restored using SQL scripts

1. Recovery Solution should be installed again if its installation was corrupted.
2. Should be executed either `Restore_All_RS_Clusters.sql` or `Restore_Single_RS_Cluster.sql` scripts (see [Notification Server Database Backup](#) on page 58) depending on whether you want to restore all Recovery Clusters or just one. Note that in case of using `Restore_Single_RS_Cluster.sql` script admin should specify correct RS Cluster GUID in the script.
3. Recovery Solution SQL database should be restored using SQL Server tools. For information, see [Recovery Database Restore](#) (page 62).
4. Recovery Solution data files should be restored from backup to original location. See [Data Files Restore](#) (page 62).
5. Recovery Server should be installed to the same machine where it was originally installed.

6. If Recovery Database created on different SQL server than Notification Server database, then saved ODBC DSN string should be restored as well.
7. You should also restore the AeXRSDatabaseUser account backed up at step [AeXRSDatabaseUser login account](#) (page 58) if it is missing.

Notification Server Database Restore

If the whole Notification Server Database was backed up, it can be restored using approach described in [Recovery Database Restore](#) on page 62. Simply substitute the Notification Server Database name instead of Recovery Database name.

If either of backup SQL scripts was used, then the appropriate restore script should be used to restore either all or a specific Recovery Cluster.

Data Files Restore

If data files mirroring is utilized in Recovery Solution 7.0 installation, then it's only needed to restore the files to the main storage group. Other groups will be synchronized, either (for synchronous groups) automatically on the background or (for asynchronous groups) during the next synchronization job.

We recommend that you back up the data files along with the Recovery Database, and also restore these two pieces of information together.

Recovery Database Restore

This section describes how to restore the database from a backup. For instructions on creating a backup, see [Recovery Database Backup](#) on page 59.

The following instructions help you restore the Recovery Database. For additional information on backup and restore of Microsoft SQL Server databases, see Microsoft SQL Server documentation.

To restore the database

1. Install the Recovery Server.
2. Stop the Recovery Server service.
See "Stopping and Starting the Recovery Server Service" in the *Recovery Solution User's Guide*.
3. If the server is running Microsoft SQL Server:
 - a. Open SQL Enterprise Manager.
 - b. In the Console Tree (usually on the left side), expand SQL Server Group, the name of the server, and then Databases.
 - c. Select the database for Recovery Solution.
By default, it is named AeXRSDatabase.
 - d. In the Details Pane, under Backup, click Restore database.
 - e. For Restore, click From device, then click Select Devices.
 - f. For Restore from, click Disk, then click Add.
 - g. Specify the file name of the backed up database, then click OK.

Chapter 6

Recovery Agent Troubleshooting

To troubleshoot the Recovery Agent, choose the troubleshooting topic that applies to your situation.

- [Troubleshooting: Install/Uninstall](#) on page 64
- [Troubleshooting: Snapshots](#) on page 65
- [Troubleshooting: Restoring Data](#) on page 71
- [Troubleshooting: Error Messages](#) on page 75
- [Troubleshooting: Options](#) on page 77
- [Troubleshooting: Event Logs](#) on page 79
- [Troubleshooting: Rollback](#) on page 79
- [Troubleshooting: Other Issues](#) on page 81

Troubleshooting: Install/Uninstall

What type of installation problem are you having?

- I cannot update my Recovery Agent installation. See [Troubleshooting: Cannot Update Recovery Agent](#) on page 64.
- When I update Recovery Agent, my settings are lost. See [Troubleshooting: Settings Not Saved During Update](#) on page 65.
- When Installing Recovery Agent fails with error “unable to configure the settings. See [Troubleshooting: Install fails with unable to configure the settings error](#) on page 65

Troubleshooting: Cannot Update Recovery Agent

The following are some potential causes of update problems.

- If the automatic update doesn't seem to work, make sure that you are logged on as an authorized user of Recovery Solution, then let the upgrade run again. You can cause the upgrade to start by simply browsing your protected files.
- To install the Recovery Agent on a Windows 2000/XP computer, you must be a member of the Administrators user group or have administrative rights on your computer. If you don't have administrative rights, ask the Recovery Solution administrator to install the software for you.
- If you get errors trying to install the Recovery Agent over an older version, try uninstalling the Recovery Agent first, then install the new version.

In some cases Setup might prompt for a user name and password, but not accept them even if they are valid. This could occur if you are trying to reinstall from a command-line Setup package provided by your administrator, and you are not the original user who installed Recovery Agent on your computer. In this case, you need to specify user credentials on the command line as follows:

```
AgentSetup.exe /Reinstall /Comp:computer /User:primary_username /
GUser:your_username /Pass:your_password
```

If your administrator provided other command-line switches to use, be sure to include them as well. The order that switches appear on the command line is not important.

Troubleshooting: Settings Not Saved During Update

During a regular software update or reinstallation using the same account, all your settings should be saved. However, some settings might revert back to the default state under any of the following circumstances.

- You completely uninstall the software first, then reinstall it.
Uninstalling the software removes all settings. If you want to update the software and keep your old settings, simply install it over the existing copy.
- You install the software on a different computer from the one you originally installed it on.
Some settings are stored on your computer rather than on the server, so even if you use the same account, those settings are not kept when you install the software on a different computer.

Troubleshooting: Install fails with unable to configure the settings error

During install you get the following error:

Error 25015. The setup has detected that Recovery Agent is unable to configure the settings for this computer. See more details in to the AexCRAS.log file which is available in your Windows temporary folder.

The reason for this error is that the current logged in user on the computer can not access or modify settings in the registry, the user can try the following steps to correct the issue:

1. Run **Regedit**
2. go to the following entry
HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Express
3. right click on **Express** folder and select **Permissions....**
4. Reset Permissions for all users to Full Control and Read
5. Rerun the Recovery Agent install

Troubleshooting: Snapshots

What happens when you try to take a snapshot?

- The snapshot options are disabled or otherwise not available. See [Troubleshooting: Snapshot Options Unavailable](#) on page 66.
- I start a manual snapshot, but nothing happens. See [Troubleshooting: Nothing Happens](#) on page 66.

- I start a manual snapshot, but my computer locks up or otherwise fails to respond as expected. [Troubleshooting: Erratic Behavior](#) on page 67.
- I scheduled a timed or automated snapshot that does not appear to have been performed. See [Troubleshooting: Snapshots Don't Run](#) on page 67.
- The snapshot starts correctly, but stops before it is completed. See [Troubleshooting: Snapshot Stops Prematurely](#) on page 69.
- During the snapshot, the Windows Installer screen appears. See [Troubleshooting: Windows Installer Appears During Snapshots](#) on page 70.
- The snapshot does not contain all my files. See [Troubleshooting: Snapshot Is Missing Files](#) on page 70.
- I receive an error message while the snapshot is being taken. See [Troubleshooting: Error Messages](#) on page 75.
- I am prompted to log on, but then nothing happens. See [Troubleshooting: Logon Problems](#) on page 83
- I am prompted to log on, but my user name and password are not accepted. See [Troubleshooting: Logon Problems](#) on page 83.

Troubleshooting: Snapshot Options Unavailable

- An administrator can disable snapshot and recovery activity on your computer. This might be done temporarily for maintenance purposes.
- If you want to take a snapshot of a specific file or folder, and you browse to the folder using Windows Explorer, you can start a snapshot by right-clicking the file or folder and clicking **Snapshot** from the menu. You can also select the file or folder and click **File > Snapshot**. In some cases, the Snapshot option is not available. This problem can occur if using a version of Windows Internet Explorer earlier than 6.0. To solve this problem, upgrade Internet Explorer to 6.0 or newer.

Troubleshooting: Nothing Happens

If you choose an Recovery Solution option but nothing happens, it could be for the following reasons.

- Under some circumstances, if you are starting a snapshot or restore, it might take up to several minutes for the progress window to appear, so it seems as if nothing is happening.
- If for some reason the server is not working properly, it might also be several minutes before an error message appears.

You can check the availability of the server by looking at the Windows taskbar. The Recovery Agent system tray icon, usually located at the bottom right of your screen, displays a red mark if there is a problem contacting the server.

- If the server is unavailable, contact your Recovery Solution administrator for further assistance.
- If the server is available, there might be a configuration problem. See [Troubleshooting: Options](#) on page 77.

If the progress window opens but does not continue, see [Troubleshooting: Recovery Solution Stops During a Snapshot or Restore](#) on page 69.

- If you are using Windows XP and your computer is not part of a Windows domain, you might be running into problems with Fast User Switching. For more information, see [Troubleshooting: Fast User Switching](#) on page 84.

Troubleshooting: Erratic Behavior

There appear to be some incompatibilities between Recovery Agent and other products that could cause some Recovery Solution functions to fail. Check to see if you have the programs below installed. If you do, you might need to uninstall the other product before you can continue.

- Legato Replica
- Replica for HP SureStore Tape
- Stac Replica Tape
- Timbuktu Enterprise 2.0 Build 635
- Tivoli Data Protection for Workgroups

Troubleshooting: Snapshots Don't Run

Snapshots can be performed at specific times (scheduled), or they can be associated with specific events (Example: snapshots that start when you log off).

What type of snapshot are you having trouble with?

- Scheduled snapshots. See [Troubleshooting: Scheduled or Automated Snapshot Doesn't Run](#) on page 67.
- Snapshot on logoff. See [Troubleshooting: Snapshot on Logoff Doesn't Run](#) on page 68.

Troubleshooting: Scheduled or Automated Snapshot Doesn't Run

Automated snapshots can be performed at specific times (scheduled), or they can be associated with specific events (Example: snapshots that start when you log off). There are a number of reasons that a scheduled or automated snapshot might not start when you expect it to.

If a scheduled or automated snapshot does not run, check the following.

- Scheduled snapshots that are based on a time of day take place according to the internal clock of the server, not your computer. When scheduling your snapshots, you should allow for typical deviations in clock settings.
Example: suppose your computer's clock reads 1:00 P.M., while the server's clock reads 1:10 P.M. If you schedule a snapshot to start at 1:05 P.M., you might expect it to run in 5 minutes, but it won't because according to the server 1:05 P.M. is already past. The snapshot won't run until the next scheduled day.
For proper operation, the clocks on the Recovery Servers and clients must be synchronized.
- Your computer might have been off. You do not have to be logged on with a user name and password, but your computer must be on for a snapshot to be run.

- To ensure that all your files are protected, you should reinstall the software as soon as possible after an upgrade to Windows. If you don't reinstall, then your scheduled or automated snapshots might not occur.
- The Recovery Solution administrator can limit the number of simultaneous connections to the server. If many scheduled snapshots are running at the same time, then some snapshots might get delayed because they are not all allowed to run at the same time. As long as the server is not constantly using the maximum number of connections throughout the entire scheduled time range for your snapshot, the snapshot should start (though probably not at the beginning of the time range).

On the other hand, if many other protected computers are accessing the server constantly during the entire time range scheduled for your snapshot, the scheduled snapshot might not run on that day, and your computer won't take an automatic snapshot again until the next scheduled snapshot time. If you are allowed to change your own snapshot schedule, you can increase the time range to give your snapshot a greater chance of being taken.

If your snapshots are frequently skipped because of limited access to the server, you should notify the Recovery Solution administrator.

- If there's a problem on the server or if the server is simply not running during your scheduled snapshot time, the snapshot won't start.

Troubleshooting: Snapshot on Logoff Doesn't Run

Snapshot on logoff might not run for the following reason.

- Windows might be logging you off before the snapshot has a chance to run. This behavior is controlled with an application timeout registry setting that is different for each user on the computer.

In most versions of Windows, the default for this timeout is long enough that it does not interfere with the snapshot on logoff timeout. However, in Windows XP and Windows 2000, the default timeout is too short. Recovery Solution automatically increases this timeout when Setup is run, but if the setting was subsequently changed, or if you are not the user who installed the software, then you might have to change the setting manually.

To increase the Windows application timeout

1. From the Windows Start menu, click **Run**.
2. Type `regedit.exe`, and click **OK**.

Caution

Be extremely careful when editing the Windows registry. If you accidentally change or delete the wrong values, your computer could stop working properly. You might want to print the Registry Editor Help topic "To restore the registry" before making any changes. This topic describes how to revert to an old version of the registry if your computer won't start.

3. Browse to the following Registry location.
`HKEY_CURRENT_USER\Control Panel\Desktop`
4. In the list of values (usually on the right), select **HungAppTimeout**.
5. From the Edit menu, click **Modify**.

6. Under **Base**, click **Decimal** so you can enter the number you want in regular decimal format.
7. Under **Value data**, specify the number of milliseconds you want Windows to wait before automatically trying to close an application.

Be sure this value is at least 20000.

8. Click **OK**.

For additional troubleshooting information, see [Troubleshooting: Snapshots Don't Run](#) on page 67.

Troubleshooting: Snapshot Stops Prematurely

What happens when the snapshot stops?

- The Progress window stays on the screen for a long time without continuing. See [Troubleshooting: Recovery Solution Stops During a Snapshot or Restore](#) on page 69.
- Recovery Solution completes the snapshot, but the snapshot does not contain all of my files. See [Troubleshooting: Snapshot Is Missing Files](#) on page 70.
- Recovery Solution stops the snapshot and displays an error message. See [Troubleshooting: Error Messages](#) on page 75.
- The Progress window closes. See [Troubleshooting: Unknown Solution](#) on page 84.
- Something else happens. See [Troubleshooting: Unknown Solution](#) on page 84.

Troubleshooting: Recovery Solution Stops During a Snapshot or Restore

- If you're running a snapshot, check to see if the **Close** button is available. When a snapshot is complete, the **Close** button replaces the **Stop** button, and a Snapshot complete message appears. Sometimes the statistics mistakenly indicate that there is still more information to be copied, but this is not the case. Once the **Close** button becomes available, all files have been successfully included in the snapshot.

Note

Be careful not to close the window too soon. If you are running a snapshot on multiple drives, the progress is displayed separately for each drive and reaches 100% after each drive is finished. If more data still needs to be included, the button reads **Stop**, not **Close**, and if you choose it, the rest of the files will not included.

- If you start a snapshot and the **Close** button becomes available but no files appear to have been protected (the percentage complete stays at 0%), you might be using the McAfee VirusScan Safe & Sound feature. If you use this feature to store backup files as "protected volume files," your snapshots might not run successfully. The problem can be fixed by either turning off **Safe & Sound**, or by reconfiguring it to store backups as folders instead.
- If you are restoring many files, the message "Initializing the list of items to restore. Please wait..." might stay on the screen for a very long time. This is normal behavior. You can continue working in other programs while the restore process initializes.

- If you think your snapshot or restore is really stalled, try clicking the **Stop** button in the **Progress** window. (If you don't see a **Stop** button but you see a **Close** button, then the snapshot or restore is finished, and you can close the window.)
If you cannot close the Progress window, close your other programs and restart your computer, then try the snapshot or restore again. If it still fails, contact the Recovery Solution administrator. There might be a problem with the server.

Troubleshooting: Windows Installer Appears During Snapshots

You might see the Windows Installer screen appear during your snapshots if you have Microsoft Office 2000 installed on your computer, and any of its components are configured with the option to **Install on first use** (which is the default for many components).

If you cancel the installer, the snapshot should continue normally.

Troubleshooting: Snapshot Is Missing Files

Listed below are some reasons that your snapshots might be missing files.

- The files are excluded from the snapshot.
A file might be excluded from a snapshot in any of the following ways.
 - By not including the drive in the snapshot.
If performing a manual snapshot, make sure you select the drive on which you want to run a snapshot.

For scheduled snapshot, make sure the drive is checked in the snapshot schedule options.
 - By excluding the file automatically from all snapshots (manual or scheduled).
This is configured in the snapshot exclude options.

There are a number of ways you that the exclude options might be configured to make Recovery Solution ignore a file during a snapshot. For more information, see the "Snapshot Exclusion Notes" in the *Recovery Solution User's Guide*.
- The files are open or locked during snapshot.

Under certain conditions, Recovery Agent fails to backup files, which are locked or open. These conditions include the following:

- OFM synchronization fails during snapshot.
Sometimes, when the write activity rate spread is uneven among the protected computer multiple hard drives, the most active drive's write operations may cause OFM synchronization to fail even though this particular drive was excluded from the snapshot. In this case, you need to change the OFMState value to enable OFM synchronization by volume (as opposed to the default "synchronize the whole system" setting).

Warning

Before using "Sync by volume" option, make sure there are no databases or applications that span across multiple volumes in your environment.

- If you start a snapshot and the **Close** button becomes available but no files appear to have been protected (the percentage complete stays at 0%), you might be using

the McAfee VirusScan Safe & Sound feature. If you use this feature to store backup files as "protected volume files," your snapshots might not run successfully. The problem can be fixed by either turning off Safe & Sound, or by reconfiguring it to store backups as folders instead.

Troubleshooting: Restoring Data

Which type of data restore are you trying to perform?

- I am trying to restore files by browsing my snapshot data. See [Troubleshooting: File Restores](#) on page 71.
- I am trying to perform a rollback. See [Rollback troubleshooting](#) (page 102).
- I am trying to perform a Full System Recovery. See [Full System Recovery troubleshooting](#) (page 95).
- I am trying to restore files with a Web browser. See [Troubleshooting: Web-Based File Recovery Logon Doesn't Appear](#) on page 73.
- I don't know the difference between the restore types. See [Troubleshooting: Unknown Restore Type](#) on page 74.
- [Other Issues Relating to Restoring Data](#) on page 74

Troubleshooting: File Restores

What happens when you try to restore data?

- I cannot view my protected files. See [Troubleshooting: Cannot View Protected Files](#) on page 72.
- I'm having trouble understanding file versions or getting a particular file version. See [Troubleshooting: Protected File Versions](#) on page 72.
- I choose **Restore** or drag file snapshots to my computer, but nothing happens. See [Troubleshooting: Nothing Happens](#) on page 66.
- I am prompted to log on, but then nothing happens. See [Troubleshooting: Logon Problems](#) on page 83.
- I am prompted to log on, but my user name and password are not accepted. See [Troubleshooting: Logon Problems](#) on page 83.
- I cannot log on with a different account when using Web-based file recovery. See [Troubleshooting: Web-Based File Recovery Logon Doesn't Appear](#) on page 73.
- Windows Explorer crashes. See [Troubleshooting: Restore Crashes Windows Explorer](#) on page 73.
- Recovery Agent freezes during a search for files to restore. See [Troubleshooting: Recovery Solution Freezes During File Search](#) on page 74.
- I choose **Restore**, but my computer locks up or otherwise fails to respond as expected. See [Troubleshooting: Erratic Behavior](#).
- The restore process starts correctly, but stops before it is completed. See [Troubleshooting: Restore Stops Prematurely](#) on page 74.
- I receive an error message during the restore process. See [Troubleshooting: Error Messages](#) on page 75.

- I cannot restore a file larger than 4GB on a FAT32 disk. See [Troubleshooting: Not Enough Space Available to Restore \(FAT32\)](#) on page 73.
- I completed a manual restore, but some of the files I tried to restore are missing or damaged. [Troubleshooting: Unknown Solution](#) on page 84.

Troubleshooting: Cannot View Protected Files

The following are potential causes of this problem.

- If a particular file or folder originated on an NTFS drive, and you do not have at least read access to the file or folder, then you cannot see it in the list of protected files. However, if you restore a folder containing the secure item, the item will also be restored (but you still won't have access to open it).
- It's possible that your account has been locked out from the server. Possible symptoms of this problem include the following.
 - You cannot expand the Client Recovery Agent folder in Windows Explorer.
 - Trying to open the Client Recovery Agent folder in its own window causes Windows to display an Action canceled Internet Explorer page.
- If you are using Windows XP and your computer is not part of a Windows domain, you might be running into problems with Fast User Switching. For more information, see [Troubleshooting: Fast User Switching](#) on page 84.

Troubleshooting: Protected File Versions

What type of file version problem are you having?

- I don't know how to find the version I need. See [Troubleshooting: Cannot Find File Versions](#) on page 72.
- I cannot tell the difference between file versions. See [Troubleshooting: Protected File Versions Are the Same](#) on page 72.
- I have a different problem. See [Troubleshooting: Miscellaneous File Version Problems](#) on page 73.

Troubleshooting: Cannot Find File Versions

While browsing protected files, you can change which file versions are displayed by clicking the **View** menu, then **Recovery Solution Versions**.

For details about the view options, see "Viewing and Restoring Protected Files" in the *Recovery Solution User's Guide*.

Troubleshooting: Protected File Versions Are the Same

If you are viewing multiple versions of your protected files and you encounter two or more files that appear to be identical, look at the **Snapshot Taken** column. The date and time shown here might be the only distinguishable difference between versions of a file. This could happen if the file itself did not change between snapshots, but the properties of the file did. Example: Recovery Solution creates a new version of the file if the only change is in its NTFS security attributes.

In most cases, you'll probably want to restore the file that has the latest snapshot date.

Troubleshooting: Not Enough Space Available to Restore (FAT32)

If you try to restore a file larger than 4 GB on a disk formatted with FAT32 file system, you will receive the error "Not enough space available to restore file" even though there may be enough free space available on the disk. This is a limitation of the FAT32 file system. The largest possible file for a FAT32 volume is 4 GB minus 2 bytes.

Troubleshooting: Miscellaneous File Version Problems

For details about the view options, see "Viewing and Restoring Protected Files" in the *Recovery Solution User's Guide*.

Troubleshooting: Web-Based File Recovery Logon Doesn't Appear

Under some circumstances, Web browsers can obtain valid logon credentials without prompting you. This could make it difficult for you to access protected files that are stored under an account name that is different from the one the browser automatically obtains.

The Web-based file recovery logon prompt might not appear if any of the following conditions are true.

- You have already accessed Web-based file recovery during the same Web browser session.

Even if you choose the **Log Off** button, your logon credentials are not necessarily cleared from the browser's cache, so returning to the page might not require another logon.

- You are running Internet Explorer, and your logon credentials for Windows are the same as those for Recovery Solution.

In this case, Internet Explorer just uses your Windows user name and password without prompting for a logon.

If a logon prompt is required (Example: if you want to access protected files that are stored under a different account name), then you can do one of the following.

- Log onto Windows with a different user account.
- Access Web-based file recovery using Netscape, which is available for free from the Netscape Web site.

Troubleshooting: Restore Crashes Windows Explorer

There appears to be a compatibility problem between Recovery Solution and a program called PowerArchiver. If PowerArchiver is installed, you might need to disable its Explorer shell extension feature before you can restore files.

To disable the PowerArchiver shell extension, do the following.

1. Open PowerArchiver.
2. Click **Options**.
3. Click **Configuration**.

4. Click the **Explorer Shell Extensions** tab.
5. Clear the **Use Explorer Shell Extensions** checkbox.
6. Click **OK**.

Troubleshooting: Recovery Solution Freezes During File Search

If you are searching for files to restore and the Recovery Agent freezes, it may be because the search operation was interrupted and then restarted. In this case, you may need to restart your computer in order to continue using Recovery Solution.

Troubleshooting: Restore Stops Prematurely

What happens when the restore stops?

- Recovery Solution stops the restore and displays an error message. See [Troubleshooting: Error Messages](#) (page 75).

Troubleshooting: Unknown Restore Type

You can restore data in the following ways.

- **Regular Restore**

You are performing a regular restore if your computer works, but you have lost some identifiable data that you need to retrieve from a snapshot. You are browsing your snapshot and restoring the files you need.

- **Rollback**

You are performing a rollback if you can start your computer, but it is not working properly and you want to return it to a previous state.

- **Full System Recovery**

You are performing a Full System Recovery if your files have become so damaged that your computer no longer works properly, and you have lost most or all of your data. You are restoring files by using a Full System Recovery disk created for you by the Recovery Solution administrator.

Which type of data restore are you trying to perform?

- I am trying to restore files by browsing my snapshot data. See [Troubleshooting: File Restores](#) on page 71.
- I am trying to perform a rollback. See "Performing Rollbacks" in the *Recovery Solution User's Guide*.
- I am trying to perform a Full System Recovery. See "Recovery Solution Full System Recovery" in the *Recovery Solution User's Guide*.

Other Issues Relating to Restoring Data

Custom user names for message queues gets renamed into the GUID-like names

Sometimes after a rollback or full system recovery, the custom user names for the message queues get renamed into GUID-like names. Such names will be returned back

to the normal view after the user sends a new message into the queue or after restarting the Message Queueing service.

Troubleshooting: Error Messages

Where do you see this error message appear?

- The message appears in the Progress dialog box. See [Troubleshooting: Error Messages in the Progress Dialog Box](#) on page 75.
- The message pops up in its own window. See [Troubleshooting: Error Message Boxes](#) on page 76.
- I found the message in the event logs. See [Troubleshooting: Error Messages in the Event Logs](#) on page 79.

Troubleshooting: Error Messages in the Progress Dialog Box

If the message says that there was an error restoring the registry, see [Troubleshooting: System Low on Registry Quota](#).

Otherwise, have you previously performed the same task without seeing this error?

- Yes, I was once able to perform this task successfully. See [Troubleshooting: New Error](#).
- No, this error often appears when I perform this task. See [Troubleshooting: Repeated Error](#).

Troubleshooting: New Error

A new error indicates that something on your computer, on the server, or on the network has changed recently.

- First, try again. Sometimes temporary conditions on the network prevent normal communications from occurring, and a retry is all that's required. You might also find that restarting your computer makes the problem disappear.
- If you recently changed any settings (particularly network settings) or installed any new software on your computer, it's possible that Windows replaced some of the shared files required by Recovery Agent. If the files were replaced with older versions, then Recovery Agent might no longer work properly. Specifically, some programs replace the DCOM system files that Recovery Solution uses to communicate between your computer and the server, which could prevent you from running snapshots and restoring data. Ask your Recovery Solution administrator to help you get the correct files back on your computer.

Note

To minimize this problem, always keep the newer versions of files when given the choice. Windows usually asks whether or not you want to keep your existing version of a file when it is newer than the one being installed, and you should always choose Yes. Some programs replace files without asking, so you might still see this problem occasionally.

- If you recently installed FrontPage 98 Personal Web Server, you might need to change one of the default Personal Web Server settings to allow you to continue

taking snapshots manually. For instructions, see [Troubleshooting: FrontPage 98 Personal Web Server Conflict](#) on page 82.

- If any network settings changed recently, Recovery Solution might not have the information it needs to communicate properly across the network. If you changed the network configuration of your own computer, you might try putting your settings back the way they were to see if it fixes the problem. If you're running certain versions of Windows, you can use Recovery Solution to do this. For details, see "Saving and Restoring Network Settings" in the *Recovery Solution User's Guide*.
If your network administrator changed settings somewhere else on the network, or if anything on the Recovery Server was changed, you might ask if other Recovery Solution users are encountering problems as well. If they are, there's a good chance that the network change has something to do with the problem. You'll have to work with the network administrator or the Recovery Solution administrator to correct the problem.

For more recommendations, see [Troubleshooting: Error Checklist](#) on page 79.

Troubleshooting: Repeated Error

- If you haven't restarted your computer in a long time, restart it and try again. Sometimes restarting the computer clears temporary problems from memory.
- If you haven't successfully run a snapshot yet, try reinstalling Recovery Agent using your existing account.
- If you have FrontPage 98 Personal Web Server installed, you might need to change one of the default Personal Web Server settings to allow you to take snapshots manually. For instructions, see [Troubleshooting: FrontPage 98 Personal Web Server Conflict](#) on page 82.

For more recommendations, see [Troubleshooting: Error Checklist](#) on page 79.

Troubleshooting: Error Message Boxes

Here are some specific types of error messages that you might see. For information about solving each problem, follow the appropriate link.

- The message says that the job could not be submitted. See [Troubleshooting: Job Could Not Be Submitted](#) on page 77.
- The message says that my computer's drive configuration has changed, but it hasn't. See [Troubleshooting: Drive Configuration Message](#) on page 77.
- The message says that the system is running low on registry quota. See [Troubleshooting: System Low on Registry Quota](#) on page 77.
- My virus protection program warns me about changes to my computer. See [Troubleshooting: Virus Warning During Rollback](#) on page 80.
- The message indicates a problem with an "authentication service." See [Troubleshooting: Options](#) on page 77.
- The message indicates an error in the module tapeng.exe.

If your error message does not appear above, have you previously performed the same task without seeing this error?

- Yes, I was once able to perform this task successfully. See [Troubleshooting: New Error](#) on page 75.

- No, this error often appears when I perform this task. See [Troubleshooting: Repeated Error](#) on page 76.

Troubleshooting: Job Could Not Be Submitted

In Windows 2000/XP, one cause of this error is that the drive that contains the files you are protecting or restoring uses the NTFS file system, and the local SYSTEM account on your computer does not have full access to the drive. Recovery Solution uses this account to read and write data.

To fix the problem, you need to give the SYSTEM account access to the drive. For information on modifying security settings to a drive, see Windows Help.

Troubleshooting: Drive Configuration Message

Recovery Solution detects when your computer's drive configuration has changed and informs you of this because you might need to check your settings in order to ensure that all your files are protected under the new configuration.

It is possible that configuration changes could occur that cause Recovery Solution to display this message even though no real changes to your drive configuration have been made. One circumstance under which this could occur is if you are using the McAfee VirusScan Safe & Sound feature to store backup files as "protected volume files." In this configuration, McAfee creates a virtual drive on your computer. Although this "drive" does not contain any data that needs to be protected (since it's all stored in McAfee's backup file), it causes Recovery Solution to display the drive configuration message. The problem can be fixed by either turning off Safe & Sound, or by reconfiguring it to store backups as folders instead.

Troubleshooting: System Low on Registry Quota

Under Windows 2000/XP, Recovery Solution requires that a certain percentage of the space allocated for the registry be free in order for snapshots to work. If the registry is already using most of the space available for it, then you might see this message when you perform a Full System Snapshot.

An insufficient registry quota can also prevent the registry from being restored properly.

To correct the problem, you must increase the maximum registry size so that there's enough free space for Recovery Solution to use. The change is made in the Virtual Memory dialog box along with the Windows paging file sizes.

Start by following the recommendations published by Microsoft for increasing the maximum registry size. They are included in the Microsoft Knowledge Base article Q176083, which you can obtain from a number of Microsoft technical publications or from the Microsoft Web site.

If you still encounter the error, it might be necessary to increase the maximum registry size even more. When performing a rollback, you might find you need to increase the maximum registry size to as much as 50 MB.

Troubleshooting: Options

What type of problem are you having with the options?

- I can't open the Recovery Agent Options dialog box. See [Troubleshooting: Can't Open Options](#).
- A message appears saying that my computer's drive configuration has changed, but it hasn't. See [Troubleshooting: Drive Configuration Message](#) on page 77.
- Some options don't appear and/or are disabled. See [Troubleshooting: Options Are Unavailable](#).
- A message appears saying that the schedule settings cannot be displayed. See [Troubleshooting: Schedule Settings Cannot Be Displayed](#).
- When I click the button to change my credentials, nothing happens. See [Troubleshooting: Fast User Switching](#) on page 84.
- I can't close the Recovery Agent Options dialog box. See [Troubleshooting: Cannot Access Dialog Box Buttons](#) on page 83.

Troubleshooting: Can't Open Options

What happens when you try to view the options?

- I can't find the Recovery Agent icon. See [Troubleshooting: Fast User Switching](#).
- Nothing happens. See [Troubleshooting: Nothing Happens](#) on page 66.
- I am prompted to log on, but then nothing happens. See [Troubleshooting: Logon Problems](#).
- I am prompted to log on, but my user name and password are not accepted. See [Troubleshooting: Logon Problems](#).
- I get a different error message. See [Troubleshooting: Error Message Boxes](#) on page 76.

Troubleshooting: Options Are Unavailable

Options might be unavailable for any of the following reasons.

- Your version of Recovery Agent does not include the option you are looking for.
- Your computer might not have the required support installed for an option. Example: if you do not have Dial-Up Networking installed on your computer, the options for protecting your computer remotely do not appear.
- You might not have the rights to view or change some options. By default, some options are not available to you. Also, your Recovery Solution administrator can enable or disable certain options for you.
- If you see a message saying that your schedule settings cannot be displayed. See [Troubleshooting: Schedule Settings Cannot Be Displayed](#) on page 78.
- If you are using Windows XP and your computer is not part of a Windows domain, you might be running into problems with Fast User Switching. For more information, see [Troubleshooting: Fast User Switching](#) on page 84.

Troubleshooting: Schedule Settings Cannot Be Displayed

If you see a message saying that your schedule settings cannot be displayed, it's possible that your account has been locked out from the server. If you've restarted your computer several times in a row, you might have to wait until the account lockout

expires, then restart your computer again in order to access Recovery Solution. Your administrator should be able to determine what the account lockout policy on the server is.

Troubleshooting: Event Logs

What type of problem are you having with the event log?

- After installing Recovery Agent under Windows NT, I get frequent messages informing me that the event log is full. See [Troubleshooting: Event Log Full](#) on page 79.
- I don't understand the event messages. See [Troubleshooting: Error Messages in the Event Logs](#) on page 79.
- More information: [Troubleshooting: Error Checklist](#) on page 79.

Troubleshooting: Event Log Full

Recovery Solution stores errors and other messages in the event log. Depending on how frequently you use Recovery Solution, the event log could fill up very quickly—especially if other installed programs are also writing to the same log.

You have two options for dealing with this problem.

- Clear the log each time you receive the message. You'll have the option of saving the log before you delete it.
- Change the Event Viewer settings to automatically overwrite events.
If you do this, you won't have a chance to save old log information, but in most cases it is only the recent log information that is valuable.

Troubleshooting: Error Messages in the Event Logs

See your Recovery Solution administrator for information about all Recovery Solution event messages, including errors.

Troubleshooting: Error Checklist

Here are some additional things to try if you're still receiving errors.

- Make sure the version of Recovery Agent you're running is the same as the version that's on the server. Your Recovery Solution administrator should have installation software for the correct version of Recovery Agent.

Troubleshooting: Rollback

What happens when you try to perform the rollback?

- I don't know how to perform a rollback. See "Performing Rollbacks" in the *Recovery Solution User's Guide*.
- I choose a snapshot to restore from, but nothing happens. See [Troubleshooting: Nothing Happens](#) on page 66.
- The restore process starts correctly, but stops before it is completed. See [Troubleshooting: Restore Stops Prematurely](#) on page 74.

- My virus protection program warns me about changes to my computer. See [Troubleshooting: Virus Warning During Rollback](#) on page 80.
- I receive an error message during the restore process. See [Troubleshooting: Error Messages](#) on page 75.
- I completed a rollback, but some of the files I tried to restore are missing or damaged. See [Troubleshooting: Rollback Has Missing or Damaged Files](#) on page 80.
- I completed a rollback, then I received a message saying that my computer has been disabled. See [Troubleshooting: Rollback Disables Computer](#) on page 81.
- After rolling back my system, I see an error in the module tapeng.exe. See [Troubleshooting: Rollback General Protection Fault Error Message](#) on page 81.
- After Rollback, the DHCP server was not started and error 1811 is recorded in the event log. See [Troubleshooting: DHCP Problems After Rollback](#) on page 81.
- I need to restore data, but I can't start the computer. See "Recovery Solution Full System Recovery Dialog Box" in the *Recovery Solution User's Guide*.

Troubleshooting: Virus Warning During Rollback

Some virus protection programs, such as Norton Antivirus 5.0, have an option to protect the computer's boot code. If you are running Norton Antivirus with this option turned on, and the master boot record has changed since the time of the snapshot being restored, then during the rollback Norton Antivirus prompts you to accept or reject the rollback changes to the master boot record.

No matter which option you choose, the rollback continues normally but does not restore either the master boot record or the Windows registry. If you suspect problems with the master boot record or the registry and need these files restored, you should disable the option to protect the boot code, then run the rollback (or have your administrator run it) again.

Troubleshooting: Rollback Has Missing or Damaged Files

There are some specific issues related to rolling back computers that have Microsoft Office installed.

- If you are running Microsoft Office 97, a rollback might cause the Office Shortcut Bar icons to be incorrect. (They all show the same icon.) These are caused by outdated temporary files that remain on the computer after the rollback. To correct the problem, close the Office Shortcut Bar and delete the following files from your computer. They are located in the "Office\Shortcut Bar" subfolder of the folder containing your Microsoft Office program files (by default "C:\Program Files\Microsoft Office").
 - off3071.tmp
 - off3071h.tmp
 - off3071s.tmp

Once the files have been deleted, the Office Shortcut Bar should display the correct icons.
- If you were previously running Microsoft Office 97 but upgraded to Microsoft Office 2000, you should try to avoid rolling back your computer to a point in time when

you had Office 97 installed. This might cause some Office files to be restored incorrectly. To correct the problem, you might need to reinstall Office.

- If your computer's drive configuration has changed since the time of the snapshot to which you are rolling back, then the rollback restores your old drive configuration, but it's possible that one or more of your drives contains no data after the rollback is complete. To restore the data, perform a second rollback to the same snapshot you chose for the first rollback.

Troubleshooting: Rollback Disables Computer

If you roll back to a snapshot that was performed using a previous version of Recovery Agent, your Recovery Agent software is also rolled back. To bring your system up to date, you should reinstall the software using your existing account.

Troubleshooting: Rollback General Protection Fault Error Message

Certain Toshiba DVD-ROM drives, including the Toshiba Tecra 750 DVD, include a utility called Toshiba Access Panel. Under certain situations, a minor bug in this utility causes a General Protection Fault error "in module tapeng.exe at 0137:0040d919." This error might occur after files are restored during a rollback using Recovery Solution. However, the rollback is successful; this error does not affect your data. Simply close the error message and restart the computer.

Troubleshooting: DHCP Problems After Rollback

Sometimes after a rollback is completed on the client computer, the DHCP service is not started and an error -1811 appears in event log. This can occur if during the rollback, the client computer requested the IP Address from the DHCP server. To resolve this problem, delete j50.chk from the Windows DHCP folder and then restart server or start DHCP service manually.

Troubleshooting: Other Issues

- [Troubleshooting: Cannot perform user registration or authentication](#) on page 82
- [Troubleshooting: DCOM](#) on page 82
- [Troubleshooting: FrontPage 98 Personal Web Server Conflict](#) on page 82
- [Troubleshooting: Logon Problems](#) on page 83
- [Troubleshooting: Cannot Access Dialog Box Buttons](#) on page 83
- [Troubleshooting: Connection Firewall](#) on page 84
- [Troubleshooting: Fast User Switching](#) on page 84
- [Troubleshooting: Unknown Solution](#) on page 84
- [Troubleshooting: Event Viewer](#) on page 84

Troubleshooting: Cannot perform user registration or authentication

If the Recovery Agent registration or authentication does not work, one reason may be that the user is part of the Guest domain group. Guests cannot perform any operations with the Recovery Agent.

Troubleshooting: DCOM

DCOM is a Windows component that Recovery Solution uses for communication between your computer and the server. Usually it is installed and configured automatically, and you don't have to do anything with it. However, installing or removing certain Windows components can result in configuration changes that prevent Recovery Solution from being able to use DCOM.

The specific symptoms of DCOM configuration problems are different depending on which version of Windows you are running.

Windows 2000/XP/Vista

This section describes DCOM configuration problems you might encounter under Windows 2000 and Windows XP.

Symptom

Trying to view protected files or open the options window results in the error "The authentication service is unknown (0x800706d3)."

Explanation

It's likely that the remote procedure call (RPC) locator service has been removed from your computer. This is a communication service required for proper DCOM operation.

The RPC service gets removed if you uninstall the Client for Microsoft Networks networking component.

Solution

You must reinstall Client for Microsoft Networks. To do so, see To add a network component in Windows Help.

Once it is installed, you can disable it by clearing the checkbox next to it in the list. This prevents the client component from being used, but it does not remove the RPC files that DCOM applications require.

Troubleshooting: FrontPage 98 Personal Web Server Conflict

If you have FrontPage 98 Personal Web Server installed, you might need to change the following default Personal Web Server setting to allow you to take snapshots manually.

1. From the Windows Start menu, click **Settings**.
2. Click **Control Panel**.
3. Open the **Network** applet.
4. Click **Personal Web Server**.
5. Click **Properties**.

6. Change the **Use Local Security option** to **FALSE**.
7. Click **OK**.

Troubleshooting: Logon Problems

There are a number of reasons that you might have difficulty logging onto the server.

- If you entered your user name and password and nothing is happening, it might just be taking a while. Your connection to the server depends on various conditions. If nothing happens after several minutes, see the items below.
- If your user name and password are not accepted, make sure they are correct. Passwords are case-sensitive, so "PASSWORD" is not the same as "password."
- If you keep getting prompted to reregister your computer or enter your logon information, and you are sure you have entered your user name and password correctly, it's possible that one of the following has happened:
 - The server software has been recently reinstalled. Restart your computer and try again.
 - Your account has been locked out. If you've restarted your computer several times in a row, you might have to wait until the account lockout expires, then restart your computer again in order to access Recovery Solution. Your administrator should be able to determine what the account lockout policy on the server is.
- If the administrator has upgraded the copy of the console that is installed on the server, but has not yet upgraded the server software, you'll be unable to use Recovery Solution until the administrator completes the upgrade. You might want to let the administrator know that you are having problems.
- Certain networking and security components are required to be installed on your computer in order for Recovery Agent to work correctly. For more information, see [Troubleshooting: DCOM](#) on page 82.

If you still have problems, contact your Recovery Solution administrator for help.

Troubleshooting: Cannot Access Dialog Box Buttons

The minimum screen resolution requirement for Recovery Agent is 800 x 600.

- If you are using an 800 x 600 screen resolution and displaying Large Fonts, you might need to move the Recovery Agent Options dialog box up a little bit on your screen before you can access the buttons.

To do this, click the very bottom tip of the window title bar and drag it up as far as it will go.

The buttons at the bottom should come into view.
- The 640 x 480 screen resolution is not supported.
- If you are running at this resolution, you should change to an 800 x 600 or higher resolution if possible.

If you need to access the Recovery Agent Options dialog box buttons at a 640 x 480 resolution, you can use the following shortcut keys while the dialog box is displayed.

 - ENTER to click the **OK** button.
 - ESC to click the **Cancel** button.

Troubleshooting: Connection Firewall

If you are running Windows XP, you have the option of using a built-in Windows firewall to safeguard your computer while it is connected to the Internet. Unfortunately, this firewall prevents the server from reaching your computer, meaning that some Recovery Solution functions will not work.

Recovery Solution features that do not work through a Windows connection firewall include the following.

- Scheduled snapshots.
- Rollbacks started by your administrator.

Note

Internet Connection Sharing uses the Windows firewall by default, so if you use Internet Connection Sharing then you could run into the same problem.

If you are behind a corporate firewall, or on a VPN connection to a network that has a firewall, your computer is probably protected by that firewall and you can turn your personal firewall off. Assuming that the server is on the same network, this should allow all features to work properly. See also [Firewall Configuration](#) on page 31.

Troubleshooting: Fast User Switching

If you are running Windows XP and your computer is not part of a Windows domain, then a feature known as "Fast User Switching" might be enabled on your computer. This feature lets multiple users log onto the computer simultaneously, and then the computer can be quickly switched from one user's settings to another.

Recovery Solution does not currently support this environment. We recommend that you disable Fast User Switching while Recovery Solution is installed.

If you do not disable Fast User Switching, the most noticeable issue is that only one logged-on user at a time will be able to interact fully with Recovery Solution. The other logged-on users won't see the Recovery Agent desktop and system tray icons, and might not be able to open certain Recovery Agent windows or perform manual tasks with the program. Which user is able to perform these tasks might vary depending on order in which they logged on.

Troubleshooting: Unknown Solution

Recovery Agent Help does not appear to have a solution for your problem.

If you need additional assistance, check with your Recovery Solution administrator.

Troubleshooting: Event Viewer

For more information, see "Troubleshooting the Event Viewer" in the *Recovery Solution User's Guide*.

Chapter 7

Recovery Solution Troubleshooting

This chapter includes the following topics:

- [Where to look for troubleshooting information](#) (page 85)
- [Recovery Solution installation troubleshooting](#) (page 86)
- [User account & logon troubleshooting](#) (page 91)
- [Data protection & recovery troubleshooting](#) (page 93)

Where to look for troubleshooting information

You can use Recovery Solution event logs when troubleshooting problems with Recovery Solution.

See [About Recovery Solution event logs](#) on page 85.

Be sure to also read Release Notes for important information that might not have made it into the documentation. You can also review [Product Limits](#) (page 12) to view information about a few of the things that Recovery Solution is not designed to do.

If you cannot find the information you need, you can visit the support page at www.altiris.com.

About Recovery Solution event logs

An event is an important occurrence that is caused by Recovery Solution or affects Recovery Solution in some way. Examples include security data and error messages.

Different Recovery Solution components report information in several log files.

- Recovery Solution Setup, Recovery Cluster Creation Wizard and the Symantec Management Console log their events into the Altiris log.
You can view this log using the Altiris Log Viewer application on the Notification Server computer.
- Recovery Agent Setup logs events into the agent installation log (AexCRAS.log).
You can find this log on the client computer in the *%ProgramFiles%\Altiris\Recovery Agent* folder.
- Recovery Server Setup logs events into the server installation log (AexCRSS.log).
You can find this log on the Recovery Server computer in the *%ProgramFiles%\Altiris\Recovery Solution\Server* folder.

Both Recovery Solution and Recovery Agent write events to the Windows Application event log. System events might also affect or be affected by Recovery Solution.

See [Viewing events](#) on page 86.

Viewing events

Viewing the appropriate event logs is a good way to help troubleshoot Recovery Solution. You should make a note of the information that gets logged when problems occur. This information can greatly assist systems engineers and any other technical support staff you might contact for help.

If an event reported by Recovery Solution is associated with a system event reported by Windows or an operating system component, then the System Event Code of the Windows event is reported along with the other event information. System events are documented by Microsoft. The system events associated with Recovery Solution are frequently reported by the following Windows components. The typical system event codes listed in the following table are meant only as a guide; it is possible that these components could report other codes and that these codes could be reported by other components.

Windows Components	Typical System Event Code
DCOM	Starts with 0x8004.
Windows	Starts with 0x8007.
RPC	Starts with 0x8008.

To view event messages on the Recovery Server

1. From the Windows **Start** menu, click **Administrative Tools**.
2. Click **Event Viewer**.
3. In the Event Viewer, click **Altiris Recovery Solution**.
4. View the events in the right pane of the Event Viewer.

For more information about an event, double-click it in the list.

To view event messages on a protected computer

1. Open Recovery Agent Options.
2. On the General tab, click **Events Log**.
3. In the Event Viewer, click **Altiris Recovery Solution**.
4. View the events in the right pane of the Event Viewer.

For more information about an event, double-click it in the list.

Recovery Solution installation troubleshooting

This section provides troubleshooting tips for installing the server.

Use the information in this section to solve problems you might encounter while installing or getting started with Recovery Solution.

- [Server installation troubleshooting](#) (page 87)
- [Troubleshooting user installations](#) (page 89)

Server installation troubleshooting

Choose the item that best describes the problem you are having, or scroll down to browse the information.

- [After installation, W3SVC warnings appear in System event log](#) (page 87)
- [If Recovery Server uninstall encounters an error, uninstall rollback may fail](#) (page 87)
- [Altiris Recovery Server service error message after completing a Recovery Server upgrade](#) (page 87)
- [Recovery Server upgrade hangs with "Upgrade in progress" status forever](#) (page 88)
- [Recovery Solution tasks are non-factional after aggregation of legacy servers](#) (page 88)
- [Altiris Recovery Server cannot be installed because 8.3 file names creation is disabled](#) (page 88)

After installation, W3SVC warnings appear in System event log

After Recovery Server is installed on a computer with IIS, whenever Windows is restarted the System event log on the server might log warnings that the Web shares for Recovery Solution could not be created.

In fact, the shares are created and you can safely ignore these warnings. If you would prefer to eliminate the warnings, you must edit the security properties of the shared folders to grant the computer's SYSTEM read access.

By default, the shared Web folder for Recovery Agent Setup is (on the Recovery Server computer):

C:\Program Files\Altiris\Recovery Solution\Server

and the shared Web folder for Web-based file recovery is (on the Notification Server computer):

C:\Program Files\Altiris\Recovery Solution\Web.

If Recovery Server uninstall encounters an error, uninstall rollback may fail

If Recovery Server is brought to unusable state after uninstall rollback encounters an error, you can try these steps to complete the server uninstall.

- Try uninstalling Altiris Recovery Server via Control Panel > Add/Remove Programs on the Recovery Server computer.
- Initiate Recovery Server Install on the same machine from Altiris Console and try uninstalling later again.

Altiris Recovery Server service error message after completing a Recovery Server upgrade

After the setup program for Recovery Server is complete, you see the following error message in the server event log: "Service 'Altiris Recovery Server' (Altiris Recovery

Server) could not be installed. Verify that you have sufficient privileges to install system services.”

You should check the AeXCRSS.log file created by the server installation for the following message: "Setup has detected that version of selected Altiris Recovery Cluster is older than version of this Recovery Server installation package.”

See [About Recovery Solution event logs](#) on page 85.

The error may occur, if the Microsoft Services MMC snap-in window was open on the server during upgrade. This causes upgrade to fail when replacing the Recovery Server service components. If this occurs, close the Services window and other running applications on the server and retry running the Recovery Server Install.

Recovery Server upgrade hangs with “Upgrade in progress” status forever

After starting Recovery Server upgrade never ends as the server status is shown as "Upgrade in progress" on the Recovery Servers in this Cluster page. Accelerate Scheduled Snapshot and Full System Recovery Wizard functionalities may fail with error saying that no available server is found.

The problem may appear if Recovery Server upgrade occurs while Notification Server is offline.

The workaround for this problem is to uninstall the Recovery Server for which the status cannot be updated and to install it again using the corresponding policies.

Recovery Solution tasks are non-functional after aggregation of legacy servers

Recovery Solution tasks (such as Manage Protected Data, Disable or enable account, Full System Recovery image creation) may become non-functional after an aggregation of a remote legacy Recovery Server and a Notification Server that has already been running Recovery Solution with a not yet upgraded Recovery Server. Upgrading the Recovery Server should resolve the issue.

Altiris Recovery Server cannot be installed because 8.3 file names creation is disabled

8.3 file names creation must be enabled on a computer before installing the Recovery Server, otherwise the error "Altiris Recovery Server cannot be installed because 8.3 file names creation is disabled" will appear during installation.

The '8.3 file names creation' can be enabled the following way:

Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
```

Parameter: NtfsDisable8dot3NameCreation

Type: string

Set this value to 0 to enable 8.3 name creation.

Troubleshooting user installations

Listed below are some of the potential problems users might experience when trying to install Recovery Agent.

Choose the item that best describes the problem you are having, or scroll down to browse the information.

- [Error message appears during Recovery Agent setup](#) (page 89)
- [User account not validated](#) (page 89)
- [Setup does not run properly](#) (page 90)
- [Applications will not start after agent install](#) (page 91)

Error message appears during Recovery Agent setup

Script error appears in browser when user tries to install Recovery Agent from Web-based Setup wizard

- The server might be running an earlier version of Microsoft Internet Explorer. Internet Explorer 5.0 or later is required.
- The user might be running an earlier version of Microsoft Internet Explorer. Internet Explorer 5.0 or later is required.
- If Microsoft SQL Server on the server is running under the SYSTEM account or another account that is not part of the AeXRS_Users group on the server, this user must be added to AeXRS_Users before the Web installation can be accessed. An administrator can make this change using Web Console.
- "Page not found" error appears in browser when user tries to access Altiris Recovery Agent Setup Wizard or Web Based File Recovery page on Windows 2003 Server. To resolve this problem, change the status of Active Server Pages to **Allowed** in the **Web Service Extension** list in IIS 6.0. For more information about, visit the Microsoft Support Web Site.

"Cannot read the Windows registry" error

This could happen if the Windows computer name of the server does not match the Domain Name System (DNS) host name in its TCP/IP properties. One of these names should be changed to match the other.

User account not validated

Setup package prompts for credentials but does not accept them

If the server is using Windows domain security, and the user installing the software is not a user (has never used the Recovery Agent on the computer), then the /User parameter and account credentials must be specified on the command line.

Users unable to reinstall using their previous accounts

- If the server is using Windows domain security, and the domain structure has been changed in such a way that a user's original installation account or the domain containing it has been moved or renamed, then reinstallation requires the following.

- For users reinstalling through the Web-based Setup wizard, an account with the user's original username and password must exist in the domain containing the server, or in a trusted domain.
- Under certain situations, a user might see a message saying that the installation cannot be performed because there is more than one protected computer with that user name. This could happen if the server is using Windows domain security and different accounts were reinstalled to the same computer.

To resolve the conflict, an administrator must locate the user's conflicting accounts within the console. This might be easiest to do using the Protected Users list. The administrator must then do one of the following.

- Rename the computer that is not being used for the reinstallation.
- Delete the account that is not being used for the reinstallation. This can be done by selecting the protected computer, then from the **Action** menu or the context menu, choosing Mark For Delete, then Computer Account. The account is deleted during the next deletion or server space management job.

Caution

Deleting an account also deletes all protected data associated with that account.

User with expired password is prompted to change it during Web installation, but then installation stops

This appears to be an issue with the way Internet Explorer handles account authentication. If a user's password has expired, it should be changed through Windows before installing Recovery Agent.

Setup does not run properly

After user chooses to let browser run installation automatically, file downloads, but nothing happens

- Check the available disk space on the user's computer. There should be free space equal to at least 3 times the size of the installation files to allow for the creation of temporary files during the browser download and the installation.
If there is not even enough disk space to download the file, browser limitations might prevent the problem from being reported, but the installation will fail to run.
- If the user is running Windows 2000/XP, see the server detection problem description.

The automatic upgrade fails.

The following are potential causes of this problem.

- If the user who is logged on at the time the upgrade starts is not an authorized user of Recovery Solution, the upgrade might fail. To fix the problem, the user can be added to the user group for Recovery Solution (AeXRS_Users by default), or someone else can log onto the protected computer as a valid user of Recovery Solution, and let the upgrade run again. You can cause the upgrade to start by simply browsing the computer's protected files.
- The Setup files for the upgrade are downloaded to the TEMP subfolder of the installed program files folder for Recovery Agent (C:\Program Files\Altiris\Recovery Agent). If there is not enough disk space on this drive, the upgrade could fail.

- If Windows System Restore is used to return a protected computer to a point at which a previous version of Recovery Agent was installed, the automatic upgrade does not re-upgrade Recovery Solution to the current version. In this case, a reinstallation of Recovery Agent must be performed, using the computer's existing account.
- If the automatic upgrade of a Windows 2000/XP protected computer is interrupted (Example: if the computer is restarted during the upgrade), the software is unable to repair itself. If this happens, the user should reinstall Recovery Agent using the computer's existing account.
- If you are upgrading from Recovery Solution version 2.2 or earlier, and the protected computer's IP address has changed since its most recent contact with the server, then the server cannot contact the protected computer to start the upgrade. This is most likely to happen if the protected computer is configured to use a dynamic IP address. To correct the problem, an administrator can go to the server and run the "RefreshClientsIP.exe" file from the installed program files folder. This updates the IP addresses of all protected computers in the database. If the upgrade is being done gradually (a few computers at a time), the program can be run as many times as needed until all protected computers have been upgraded. Before running it, the administrator must make sure that (1) the server specifies the correct settings for your DNS server in its TCP/IP properties (if applicable), and (2) each protected computer's DNS host name matches its Windows computer name. Alternatively, a user at a protected computer can start a snapshot manually, which will cause the protected computer to send its updated information to the server.

After reinstallation from command line, Recovery Agent does not work

This can occur if the server is running in Windows domain security mode, and no domain was specified as part of the installation command. In this case, it is impossible to configure Recovery Agent options or initiate a snapshot after reinstallation. To solve this problem, you can do either of the following:

- Run the installation command again as described in Recovery Agent Setup Command Line, being sure to specify the domain parameter.
- Reinstall Recovery Agent using the Web-based Setup wizard.

Applications will not start after agent install

After the Recovery Agent has been installed, the computer must be restarted. If the computer is not restarted, applications may not start properly.

User account & logon troubleshooting

This section provides information on the following topics:

- [Protected Computers Cannot Connect to Server](#) (page 91)
- [User Logon Issues](#) (page 92)
- [Protected users cannot be authenticated](#) (page 93)

Protected Computers Cannot Connect to Server

If protected computers receive errors when trying to connect to the server, check the following.

- If the address of the cluster is changed, you must change the cluster address on the general tab of the Recovery Cluster configuration page (**Configuration > Solution Settings > Incident Management > Recovery Solution > Recovery Clusters > Recovery Cluster Configuration**).
- If the protected computer connects to the server via a Dial-Up or Virtual Private Networking (VPN) connection, and any of these remote networking settings have recently changed on the computer, it might have affected the ability of the computer to communicate with the server. You can use Recovery Solution to return the settings to a previous state.

Each time a protected computer starts, Recovery Solution saves the computer's Dial-Up Networking settings in a snapshot that is stored locally on the protected computer. These settings can be restored without making a connection to the server.

To access snapshots of network settings, the user clicks Network Settings Snapshots from the context menu of the desktop or system tray icon for Recovery Solution. This opens a window from which snapshots can be managed.

Before restoring settings, it is a good idea to first save the current settings so that they can also be restored if necessary. Then any previously saved settings can be restored.

- The DCOM configuration of either the server or the protected computer might not be correct. For information about checking the DCOM configuration settings, see [DCOM Configuration](#) on page 26.
- If there is a firewall between a protected computer and the server, it must be configured to let DCOM traffic through. For documentation about DCOM and how it works with firewalls, visit the Microsoft Web site (<http://www.microsoft.com>).

User Logon Issues

Under certain conditions, Windows 2000 running on the server counts all connections from Recovery Agent as invalid logon attempts, even if the account is authenticated properly.

Depending on the account policy settings in place on the server, it is possible under these conditions for an account to become locked out without any failed logon notifications to the user. Recovery Solution connects to the server whenever Windows starts, so if the user restarts the computer several times in a short period, the limit for invalid logon attempts might be reached, and the account locked out.

Possible symptoms of this problem that might appear to the user include the following.

- Manual snapshots cannot be run. The user is prompted for logon information, but the credentials are never accepted.
- The user cannot browse protected files.
 - The main folder in Windows Explorer cannot be expanded.
 - Trying to open the protected files folder in its own window causes Windows to display an Action canceled Internet Explorer page.
- When trying to view options for Recovery Solution, the user sees a message saying that the schedule settings cannot be displayed.

If a user encounters these problems, check the System event log on the server to see if the account is being locked out. If it is, you can change the user's account so that it is not disabled and then have the user restart the protected computer.

To prevent this problem in the future, you might consider changing the account policy to allow more bad logon attempts and/or to reduce the reset time.

Protected users cannot be authenticated

Domain users become a member of the Recovery Solution user group (AeXRS_Users) by default on the Altiris Recovery Server service startup. If, for example, because of a network connection problem, your domain controller is unavailable as the service starts, then your protected users will not be able to authenticate on the Recovery Server.

To fix the problem, verify that your domain controller is available and restart the Altiris Recovery Server service.

Data protection & recovery troubleshooting

Use the information in this section to solve problems you or Recovery Agent users might encounter while protecting or recovering data.

The topics below describe specific problems you might need to resolve.

- [Snapshot & File Restore Troubleshooting](#) (page 93)
- [Full System Recovery troubleshooting](#) (page 95)
- [Rollback troubleshooting](#) (page 102)

Snapshot & File Restore Troubleshooting

The following are some specific problems that might occur during snapshots.

Choose the item that best describes the problem you are having, or scroll down to browse the information.

- [Snapshot schedule for certain computers do not run](#) (page 93)
- [User cannot log on to start snapshot](#) (page 94)
- [Job cannot be submitted](#) (page 94)
- [Protected computer drives missing from snapshots](#) (page 94)
- [User cannot browse protected files](#) (page 94)
- [User cannot access a different account via web-based file recovery](#) (page 94)
- [Snapshots fail because server clocks are not synchronized](#) (page 95)
- [General snapshot & recovery problems](#) (page 95)

Snapshot schedule for certain computers do not run

If the protected computer is running Windows XP, its connection to the server could be hampered by the Windows connection firewall, which prevents the server from reaching the computer.

If the protected computer is behind a corporate firewall, or on a VPN connection to a network that has a firewall, it is probably protected by that firewall, so the user can usually turn off the personal firewall. Assuming that the server is on the same network, this should allow all features to work properly.

Note

Internet Connection Sharing uses the Windows firewall by default, so if the protected computer uses Internet Connection Sharing then you could run into the same problem.

User cannot log on to start snapshot

For more information, see [User Logon Issues](#) on page 92.

Job cannot be submitted

- In Windows 2000/XP, one cause of this error is that the drive that contains the files being protected uses the NTFS file system, and the local SYSTEM account on the protected computer does not have full access to the drive. Recovery Solution uses this account to read and write data.

To fix the problem, make sure that the SYSTEM account has access to the drive.

- If multiple users report this problem at the same time, it might be an issue with the server. Try to restart the server.

For more information, see “Stopping and Starting the Recovery Server Service” in the *Recovery Solution User’s Guide*.

Protected computer drives missing from snapshots

If some files or drives are missing from a snapshot, it may be because the protected computer’s disk configuration changed.

If the disk configuration changes on a protected computer, Recovery Agent should be re-installed using the existing account to ensure that the updated drives are protected.

Following are some of the specific disk configuration changes that might require re-installation of the software.

- A hard drive is added to or removed from the computer.
- A drive is resized.
- A hard drive letter is changed.
- A drive’s file system is changed (Example: from FAT to NTFS).

User cannot browse protected files

For more information, see [User Logon Issues](#) on page 92.

User cannot access a different account via web-based file recovery

Under some circumstances, Web browsers can obtain valid logon credentials without prompting the user for them. This could make it difficult for the user to access protected files that are stored under a different account name.

The Web-based file recovery logon prompt might not appear if any of the following conditions are true.

- The user has already accessed Web-based file recovery during the same Web browser session.

Even if the user chooses the Log Off button, the credentials are not necessarily cleared from the browser's cache, so returning to the page might not require another logon.

- The user is running Internet Explorer, and the user's logon credentials for Windows are the same as those for Recovery Solution.

In this case, Internet Explorer just uses the Windows credentials without prompting for a logon.

If a logon prompt is required (Example: if the user wants to access protected files that are stored under a different account name), then the user can do one of the following.

- Log onto Windows using different credentials.
- Access Web-based file recovery using a FQDN, for example:
`http://myrecoveryserver.mydomain.com/WBFR`

Normally Internet Explorer displays a logon prompt when a FQDN is used.

Snapshots fail because server clocks are not synchronized

If computers' clocks on two or more Recovery Servers in a cluster are unsynchronized, snapshots may fail. You must ensure that server clocks are synchronized. If Recovery Server computer is a member of a domain, its computer clock can be synchronized automatically by a network time server. If Recovery Server computer is not a member of a domain, the computer's clock may be automatically and regularly synchronized by an Internet time server.

To quickly synchronize computer's clock with that of another Recovery Server computer, open a command prompt on the server and enter the following command:

```
NET TIME \\computername /SET
```

General snapshot & recovery problems

If the server is running MSDE (the lite version of Microsoft SQL Server), then the number of SQL Server connections used by Recovery Solution should not be set to anything greater than 5. If too many simultaneous connections are allowed, certain tasks could fail.

For instructions on setting the number of connections used by Recovery Solution, see [Licensing Recovery Solution](#) on page 44.

Full System Recovery troubleshooting

This document contains troubleshooting information you can use in case a Full System Recovery does not work properly.

For instructions on performing a Full System Recovery, see [Running Full System Recovery](#) on page 112.

Choose the item that best describes the problem you are having, or scroll down to browse the information.

- [Disk space error appears during Full System Recovery disk creation](#) (page 96)
- [Full System Recovery does not start properly](#) (page 96)

- [Error appears during Full System Recovery](#) (page 96)
- [Full System Recovery fails when creating disk structure](#) (page 99)
- [Full System Recovery incomplete, but no error appears](#) (page 99)
- [Problems occur after server upgrade](#) (page 100)
- [Recovery Agent not working after Full System Recovery](#) (page 101)
- [Files missing or outdated after Full System Recovery](#) (page 101)
- [Full System Recovery stalls](#) (page 101)
- [Full System Recovery CD-ROM failure](#) (page 101)
- [Cannot cancel restore of folder](#) (page 102)
- [Account disabled after full system recovery](#) (page 102)
- [Full System Recovery fails on HP NetServer LC2000](#) (page 102)

Disk space error appears during Full System Recovery disk creation

Make sure that the network share for Full System Recovery has free disk space equal to the total size of the CD/DVD-ROM images plus the maximum amount of data for a single CD/DVD-ROM (depending on the capacity of your blank CD/DVD media).

Full System Recovery does not start properly

Computer starts normally, but nothing else happens

After the computer starts, run the Full System Recovery program (RNDM_DR.EXE) at the command prompt.

If the program still does not start, create a new Full System Recovery disk.

Temporary operating system does not start

If the operating system appears to have been copied correctly but it does not start, it is possible that the disk partition or drive information was not restored correctly. Example: some types of computers use a special utility partition that is stored at the beginning of the hard disk. If this partition is not restored correctly, the temporary operating system might not be able to start.

To correct the problem, you can use a disk partition tool such as PartitionMagic to restore the original partitions and drive letters. After you restart the computer Full System Recovery should continue from the point at which it stopped.

Error appears during Full System Recovery

“Cannot load DOS. Press any key to retry.”

If the computer is booting from a floppy disk, the disk might be bad. Ordinarily this would be detected at the console, but if the floppy disk drive at the console is better at handling disk errors than the floppy disk drive at the protected computer is, Recovery Solution might not be able to detect the problem when you create the Full System Recovery disk.

Try creating a new Full System Recovery disk with a different floppy disk.

“VDISK memory allocator already installed. XMS driver not installed.”

You might have started the Full System Recovery by simply restarting the computer instead of turning it off. Be sure to turn the computer off to clear its memory, then with the first disk or CD-ROM inserted, turn the computer back on.

“Partition table file is invalid”

The Full System Recovery cannot continue because there is a problem with your computer’s file system.

This error usually appears if you have chosen to continue a Full System Recovery that you started previously. You might need to restart the Full System Recovery from the beginning.

“Hard disk [C:] is smaller than the original.”

The partition table cannot be restored.

The hard disks on the computer to which you are restoring data are too small to hold all of the protected data from the original hard disks. For Full System Recovery to work, the computer to restore must have at least as many hard disks as the original protected computer, and the contents of each original disk must fit entirely onto one of the restored computer’s disks.

Listed below are some specific circumstances that might cause this error to occur.

- A hard disk has been removed from the protected computer since the time of the Full System Snapshot.
- You are trying to restore to a different computer than the one from which the Full System Snapshot was run.
- The protected computer uses Windows 2000/XP disk volume sets or stripe sets. In this case, there must be physical disks on the recovered computer large enough to store the entire contents of the logical disks from the snapshot.

“Cannot open partition information file.”

Recovery Solution cannot access the information about the computer’s file system.

This might be because the data is invalid, or it might just be a temporary access problem.

You should start the Full System Recovery again. If you attempt to continue from where you left off and you still see this message, you will have to restart the Full System Recovery from the beginning.

“Invalid volume information file.”

The Full System Recovery cannot continue because there is a problem with the information about your hard drives.

This error usually appears if you have chosen to continue a Full System Recovery that you started previously. You might need to restart the Full System Recovery from the beginning.

“Cannot open volume information file.”

Recovery Solution cannot access the information about your computer’s hard drives.

This might be because the data is invalid, or it might just be a temporary access problem.

You should start the Full System Recovery again. If you attempt to continue from where you left off and you still see this message, you will have to restart the Full System Recovery from the beginning.

“Run-Time error R6003. Attempt to divide by 0”

You might see this message in the following cases.

- On computers with certain BIOS versions, if you attempt to recover from a bootable CD-ROM. Example: computers with American Megatrends AMIBIOS Version 1.00.04.DK0K cannot be recovered from bootable CD-ROM.

One possible work around is to use the console to create a bootable floppy disk, and restart the Full System Recovery from the floppy disk. However, this might not work on all BIOS versions.

“Disk Write Error. Could not write to disk %c.”

It is possible that part of the disk specified is damaged. You might try using a tool such as ScanDisk to mark the bad clusters as unusable. If there is enough disk space left over to recover the system, you can try again. Otherwise, you can install the operating system manually and perform a data-only Full System Recovery.

You could also replace the hard disk with another one that is at least the same size as the original one and then run the Full System Recovery again.

“Original boot sector not found”

You might see this message on computers with a single SCSI drive and certain BIOS versions installed, if you attempt to recover from a bootable CD-ROM. One possible work around is to use the console to create a bootable floppy disk, and restart the Full System Recovery from the floppy disk.

“ntldr not found”

If the protected computer has multiple SCSI hard disks, and the computer is configured in the BIOS to boot from one of these SCSI hard disks with an ID greater than 0, you cannot perform a Full System Recovery on the computer. If the computer will not boot, you must install the operating system manually. Then you can restore the data from the Full System Recovery CD-ROM.

“Cannot extract files to disk”

You might see this message if you are recovering from a CD-ROM set in which the temporary operating system spans more than 1 disc. To fix the problem, you must recreate the discs with a temporary operating system smaller than the capacity of a CD-ROM (650 MB). The same error can also appear in case of a bad CD media.

“The modem has detected an internal error”

You might see this message during Full System Recovery on the IBM ThinkPad 600E, along with options to restart or shut down the modem. Simply choose to shut down the modem, and the Full System Recovery should continue normally.

“D:\DISK1 is not accessible. Folder was moved or removed”

Some CD-ROM drives, notably certain NEC models, might not be able to read CD-ROMs that have not been finalized (or “closed”). If you encounter error messages claiming that files or folders cannot be found, you might need to finalize the CD-ROMs with your CD writing software.

Some CD writing programs let you finalize discs that you have already written. If you do not have this option, you must create the discs again. In that case, the easiest way to finalize the discs is to create them using the “disc-at-once” option.

System file errors

If you see Windows errors relating to system files that cannot be replaced, or Windows Update errors relating to .DLLs, you might be attempting to recover the computer from a Full System Snapshot that was performed in the middle of the installation of a program. If a user installs a program that requires the computer to be restarted, but a Full System Snapshot is performed before the computer is restarted, you cannot recover the computer from this snapshot. Try creating a new Full System Recovery disk from a different snapshot.

Service Control Manager and other Windows errors

During the Windows part of Full System Recovery, you might see error messages relating to services not starting or files not being found. Often these messages appear because certain items specified in the Windows registry were not included in the temporary operating system being used to restore the computer's files. The Full System Recovery should continue normally in the background, even if these messages appear. They should not appear when the Full System Recovery is complete.

After the temporary operating system is installed, the protected computer cannot connect to the server to complete Full System Recovery

If a network device driver was installed or updated just before the snapshot used for Full System Recovery, and the protected computer was not restarted between the driver installation and the snapshot, then it is possible that the required driver files were not included in the temporary operating system. This occurs because Recovery Solution only checks for required system files while the computer starts up. If the required files are missing, the network card might not function correctly, and a connection to the server becomes impossible.

The problem can sometimes be corrected by recreating Full System Recovery disks and adding the entire Windows folder to the temporary operating system.

"psAuthInfo or psAuthInfo->psAuthIdentityData is Null"

You might see this error if you chose a snapshot from a version of Recovery Solution earlier than 4.0 as the source for Full System Recovery. You can use snapshots from Recovery Solution 3.2 or later, but to do so you must include all user data on the CD-ROMs.

Full System Recovery fails when creating disk structure

If the Full System Recovery fails when creating the disk structure, you can perform a Full System Recovery without formatting the hard drive.

For information, see [Running Full System Recovery without formatting drives Option](#) (page 114).

Full System Recovery incomplete, but no error appears

After partitions converted to NTFS, computer restarts, but does not boot

This symptom could occur when the partition information in a disk's Master Boot Record (MBR) does not match the information in the disk controller.

To fix the problem, you need to erase the partition table from the MBR. You can use the pclean.exe program installed with the console for this purpose.

Pclean.exe is located on the Recovery Server at C:\Program Files\Altiris\Recovery Solution\Console. You can also access it through the Symantec Management Console.

To erase the protected computer's partition tables

1. Boot the protected computer to DOS.
To do this you can boot using Full System Recovery disks and then press **N** to cancel.
2. From the DOS prompt, run pclean.exe.
3. You will be prompted to enter disk numbers from which you want to erase the partition tables.
If you know which disk is causing the problem, you can erase only that partition table. Otherwise, you might have to erase them all.
4. After you have erased the partition tables restart Full System Recovery.

I'm prompted to insert next CD-ROM, but it has already been inserted, or current CD-ROM is last of recovery set

The most likely cause of this error is a bad CD. Try the following to resolve the problem.

- Click **Try Again** in the dialog box that appears following the error message.
- Recreate the CD-ROM that was being processed at the time of failure. This is not the CD-ROM that you inserted after the prompt, but the previous one. Be sure not to re-record the data onto the faulty CD-ROM. Try to continue with the new CD-ROM.

Full System Recovery stops

First make sure that the Full System Recovery has really stopped.

- Check the status messages on the screen to see if Recovery Solution is in the middle of a task.
- Check the hard disk activity light on the computer casing to see if there data is being read from or written to the hard disk.
- Even after you are convinced that the system has stopped prematurely, wait 10 minutes to be sure.

If you are still convinced that the Full System Recovery has stopped before it is done, you can try the following.

- Restart the computer. The Full System Recovery might continue normally once you restart.
- If the recovery does not continue, you might have to start over again. If you attempted a fully automatic Full System Recovery that failed, you can try a data-only Full System Recovery.

Problems occur after server upgrade

After the server has been upgraded, certain limitations of Full System Recovery may apply. If you are performing Full System Recovery over the network, you cannot use an image created with an older version of the software. In this case, the server cannot automatically upgrade the protected computer, and user's account becomes disabled.

To successfully perform Full System Recovery from an old image after a server upgrade, and ensure that the user's account remains active, use only Full System Recovery from CD-ROM (and not over the network). A similar issue arises (the user's account becomes

disabled because the new version of Recovery Agent cannot use data restored from the older version), but the user can then reinstall Recovery Agent after Full System Recovery is completed to fix the problem.

Recovery Agent not working after Full System Recovery

If Recovery Solution was uninstalled before the Full System Recovery, you might have trouble running snapshots and restoring files once the Full System Recovery is complete. That's because the uninstall process removed some of the information about the protected computer from the server.

To fix this problem, reinstall Recovery Agent using the same account as before. After the software is reinstalled, snapshots and restores should work normally.

Note

Full System Recovery can be performed from a Full System Snapshot that was done using previous versions of Recovery Solution. To use snapshots from earlier versions, you must add all the user data to the CD-ROM set.

Files missing or outdated after Full System Recovery

If you completed a Full System Recovery but some of your files are missing or outdated, the Full System Recovery disk might have been created with an older snapshot specified. Once the protected computer is up and running with Recovery Agent installed, the user can restore the missing files by using Recovery Agent options.

For more information, see the *Recovery Solution User's Guide*.

Full System Recovery stalls

If there is a large number of files on a CD-ROM recovery set, data restore may be slow, and may even appear to be making no progress for some minutes. In this case, recovery has not failed; it is simply slow.

Full System Recovery CD-ROM failure

During Full System Recovery from CD-ROM, processing of a particular CD-ROM may fail. One of the following scenarios may occur:

- During recovery, you are prompted to insert the next CD-ROM, but the CD-ROM being processed is the last in the recovery set.
- During processing of a CD-ROM, you are prompted to insert the next CD-ROM in the recovery set. Upon insertion of the next CD-ROM, recovery fails.

Try the following in order to resolve the problem:

- Click the **Try Again** button in the Recovery Solution Full System Recovery error dialog box.
- Re-record the CD that was being processed at the time of failure. This is not the CD inserted after the prompt for the next CD, but the previous one. Data from the CD being read at the time of failure must be re-recorded onto a different CD.

Cannot cancel restore of folder

Files from the folder for which you're trying to cancel the restore process are probably stored on multiple CD-ROMs. To cancel restore of the folder, you must insert and confirm cancellation for each CD-ROM containing data from that folder.

Account disabled after full system recovery

After Full System Recovery has been performed on your computer, you might see a message saying that your account has been disabled. This can happen if your computer is recovered to a point in time from before your current account status. Example: the following situations could cause this message to appear.

- You have reinstalled Recovery Agent, but your computer is recovered to a point in time before you reinstalled.
- You have uninstalled Recovery Agent, and your computer is recovered using Recovery Solution Full System Recovery.

To fix the problem, simply reinstall using your existing account.

Full System Recovery fails on HP NetServer LC2000

Full System Recovery can fail when creating disk structure on HP NetServer LC2000 with Phoenix BIOS 4.06.23 PV. For information, see [Full System Recovery fails when creating disk structure](#) on page 99.

Rollback troubleshooting

Certain error conditions that cause the rollback not to succeed might not report that condition back to the console. If the rollback seems to be running for an excessively long time, you should check the protected computer itself to see if any errors have occurred. You can cancel the job from the console job queue.

The following are some specific errors you could encounter while trying to perform a rollback.

Choose the item that best describes the problem you are having, or scroll down to browse the information.

- [Unable to see desired snapshot during a system rollback](#) (page 102)
- [Rollback cannot be started from the console](#) (page 103)
- [Job cannot be submitted](#) (page 103)
- [After rollback, user is prompted to uninstall](#) (page 103)
- [Rollback fails](#) (page 103)
- [After rollback, a restored drive contains no data](#) (page 104)

Unable to see desired snapshot during a system rollback

Problem: When the agent software is reinstalled or upgraded, the snapshots from the previous installation do not appear in the Steam Rollback wizard.

Cause: This was done by design to hide old snapshots.

Solution: You must add a registry value to use snapshots from previous installations for a System Rollback.

1. Open the Windows registry editor.
2. Browse to the following registry key:
HKEY_LOCAL_MACHINE\Software\Altiris\Express\Recovery Agent
3. Right-click on the details pane and select **New** and then **DWORD** value.
4. Type in the name `ShowRedSnapshots`.
5. Double-click **ShowRedSnapshots** and type in a value of 1.

Rollback cannot be started from the console

If the protected computer is running Windows XP, its connection to the server could be hampered by the Windows connection firewall, which prevents the server from reaching the computer.

If the protected computer is behind a corporate firewall, or on a VPN connection to a network that has a firewall, it is probably protected by that firewall, so the user can usually turn off the personal firewall. Assuming that the server is on the same network, this should allow all features to work properly.

Note

Internet Connection Sharing uses the Windows firewall by default, so if the protected computer uses Internet Connection Sharing then you could run into the same problem.

Job cannot be submitted

In Windows 2000/XP, one cause of this error is that the drive that contains the files being restored uses the NTFS file system, and the local SYSTEM account on the protected computer does not have full access to the drive. Recovery Solution uses this account to read and write data.

To fix the problem, make sure that the SYSTEM account has access to the drive.

After rollback, user is prompted to uninstall

If rollback is performed using a snapshot from an earlier version of Recovery Solution, then after the recovery is complete, Recovery Agent must be reinstalled on the protected computer with the user's existing account.

Rollback fails

The following are potential causes of this problem.

- If the server is running MSDE (the lite version of Microsoft SQL Server), then the number of SQL Server connections used by Recovery Solution should not be set to anything greater than 5. If too many simultaneous connections are allowed, certain tasks could fail.
For instructions on setting the number of connections used by Recovery Solution, see [Licensing Recovery Solution](#) on page 44.
- There might not be enough registry free space on the protected computer. Under Windows 2000/XP, Recovery Solution requires that a certain percentage of the

space allocated for the registry be free in order for snapshots or rollback operations to work. If the registry quota is insufficient, the registry cannot be restored properly during rollback.

To correct the problem, you must increase the maximum registry size so that there is enough free space for Recovery Solution to use. The change is made in the Virtual Memory dialog box along with the Windows paging file sizes. Start by following the recommendations published by Microsoft for increasing the maximum registry size. They are included in the Microsoft Knowledge Base article Q176083, which you can obtain from a number of Microsoft technical publications or from the Microsoft Web site (<http://www.microsoft.com>).

If rollback still fails, it might be necessary to increase the maximum registry size even more. You might find you need to increase the maximum registry size to as much as 50 MB.

After rollback, a restored drive contains no data

If the protected computer's drive configuration has changed since the time of the snapshot to which you are rolling back, then the old drive configuration is restored, but it is possible that one or more drives contains no data. To restore the data, perform a second rollback to the snapshot you chose for the first rollback.

Appendix A Hard Disk Support

Full System Recovery of RAIDs is supported only for a specific set of RAID adapters. See below for more information.

Notes

The full list of supported adapters can also be found in the following file:
C:\Program Files\Altiris\Recovery Agent\SCSIConfig.ini.

The latest information may be also provided in the Altiris Recovery Solution Release Notes.

For information on enabling 48-bit Logical Block Addressing (LBA) support for ATAPI disk drives in Windows 2000 and Windows XP, see Microsoft Knowledge Base articles Q305098 and Q303013 available on the Microsoft Web site (<http://www.microsoft.com>).

RAID controllers supported for Full System Recovery Converted from inset Server Raid

HP	SmartArray 641	SmartArray 5i	
Dell	CERC SATA 6ch PERC 4/DC	PERC 4e/Si	PERC 4/Di RAID
NVIDIA	SATA 4		
Silicon Image	3112A		

Index

A

- about
 - Recovery Solution 8
- access
 - problems with 92
- accounts for users 17
- AeXRSEnc utility 47
- Altiris Agent
 - about 40
 - discovering resources 40
 - installing 40

C

- client computer requirements 37
- configuration
 - of DCOM 15, 26
 - of IIS 21
 - of ODBC 25
- connection
 - troubleshooting 91

D

- database
 - errors installing 87
- DCOM 15, 26
- DCOMCNFG.EXE 27
- discovering
 - resources 40
- Distributed Component Object Model (DCOM) 15, 26
- documentation 10
- documentation resources 10
- DOS drivers
 - and recovery 12

E

- encrypted files
 - files and encryption 12
- errors
 - during Setup 87
- event log
 - configuration of 21
- event messages
 - viewing 86

F

- Full System Recovery
 - problems with 95

G

- groups

- for users 17

H

- hard drives
 - replacement of 93
- help 11

I

- Implementation Guide 10
- information about Recovery Solution 10
- installation 37, 41
 - and new hard drives 93
 - errors 42
 - of Web-based file recovery 31
 - prerequisites 37
 - problems with 89
- installing
 - Recovery Solution 41
- Internet Information Server (IIS) 21
- IP address of protected computers 34

K

- Knowledge Base 10

L

- license 44
- limits
 - of Recovery Solution 12
- logon problems 92

M

- Maximum number of threads 12
- Microsoft Internet Information Server (IIS) 21
- Microsoft SQL Server
 - and ODBC 25
- Microsoft Windows
 - and recovery 9

N

- network configuration
 - restoring 92
- network protocols
 - for DCOM communications 15

O

- Open Database Connectivity (ODBC) 25
- operating systems
 - temporary copies of 9

P

- performance
 - of recovery 14
 - of snapshots 13, 13
- performance of 14
- prerequisites 37
- problems
 - with Agent installation 89
 - with Full System Recovery 95
 - with rollback 102
 - with Setup 87
 - with snapshots 93
- protects 8
- protocols
 - for DCOM communications 15

R

- recovery 14
 - about 9
 - and disk space 13
 - and DOS drivers 12
 - over the Web 31
 - problems with 95
 - requirements for 13
- Recovery Agent
 - settings encryption utility 47
- Recovery Agent User's Guide 11
- Recovery Cluster 57, 57, 57, 57, 58, 60, 61
 - configuring 41
 - creating 41, 41
 - GUID 59
 - load balancing 61
 - Recovery Database 59
- Recovery Database 58, 61
- Recovery Server 41
- Recovery Solution
 - about 8
 - information about 10
- Recovery Solution Implementation Guide 10
- Recycle Bin 12
- Redundant Block Elimination (RBE) 13
- registry settings 12
- Release Notes 10
- remote procedure call (RPC)
 - RPC 15
- removal
 - of Recovery Solution 45
- requirements 37
- restoring files (see recovery) 9

restoring network settings 92

rollback

of network settings 92

problems with 102

S

schedules

for server jobs 35

for snapshots 92

worksheets for 35

settings

updates in database 34

setup

of Web-based file recovery 31

SIM 41, 42, 45

snapshots

performance of 13

problems with 93

speed of 13

SQL Server

and ODBC 25

Symantec Installation Manager 41

see SIM

Symantec Management Console 11,

11

Symantec Management Platform 37

system requirements 37

T

temporary operating systems 9

troubleshooting 64

Agent installation 89

Full System Recovery 95

logon problems 91, 92

rollback 102

Setup 87

U

uninstalling

Recovery Solution 45, 45

upgrading

Recovery Solution 42

user accounts

and groups 17

User's Guide 11

W

Web-based file recovery 31

Windows

and recovery 9

worksheet

job schedule 35