EMC²
RELEASE NOTES

EMC RepliStor
for Microsoft Windows
Version 6.1

Release Notes
P/N 300-002-461
Rev A01

November 19, 2005

These release notes contain information about features, system requirements, known problems, and limitations in EMC RepliStor for Microsoft WindowsVersion 6.1. The release notes supplement the *EMC RepliStor for Microsoft Windows Version 6.1 Administrator's Guide* and the *EMC RepliStor for Microsoft Windows Version 6.1 Installation Guide.*

Product Description

EMC® RepliStor® software provides real-time data replication, and increases the availability and reliability of Windows servers without the use of proprietary or specialized hardware. RepliStor software operates over both local area network (LAN) and wide area network (WAN) connections, and allows remote administration and installation. RepliStor software also operates across Windows domains; you can administer RepliStor software across domains from any RepliStor client in the network.

RepliStor software replicates files, directories, shares, and registry keys from a source system, the computer where the data that needs to be protected is located, to a target system, the computer to which the data is replicated. After an initial synchronization of the data, RepliStor software replicates any changes made to the files (or keys), transfers those changes to the target system, and updates the files on the target system.

New Features and Changes

The major new features in RepliStor Version 6.1 are:

- The ability to take VSS-compliant shadow copies of Exchange Server 2003 databases; shadow copies serve as data recovery backups on the target system. Refer to *VSS-compliant Shadow Copies* on page 3, *Taking Shadow Copies* on page 7 and *Managing Shadow Copies* on page 12, respectively.

- The addition of a simulation/reporting feature. Refer to *Simulation/Reporting* on page 14.

- The addition of mount point support on the source system. Refer to *Mount Points Supported on Source* on page 20.

These new features are described in the following sections.

VSS-compliant Shadow Copies

In RepliStor Version 6.1, you can now create and manage Exchange Server 2003 and filesystem shadow copy backups via the Volume Shadow Copy Service (VSS) framework provided by Microsoft.

VSS is a framework that integrates user applications, backup applications, and storage systems to produce consistent point-in-time data in the form of VSS shadow copies. Specifically in Replistor, VSS enables the integration of Exchange and Replistor along with third-party hardware to provide shadow copy functionality.

Shadow Copy backups of the Exchange Server 2003 database or filesystem are created on the target system in case of source system failure. The shadow copy types supported on the target include CLARiiON SnapView snapshots, Windows system shadow copies, and custom scripts.

The VSS-compliant shadow copy functionality is only supported on Windows 2003 systems.

Shadow copies allow you to obtain a consistent, restartable copy of the Exchange database or filesystem. This copy is available on the target side. If you want to perform a recovery, take the copy from the target and use it locally or copy it back to the source server and start it.

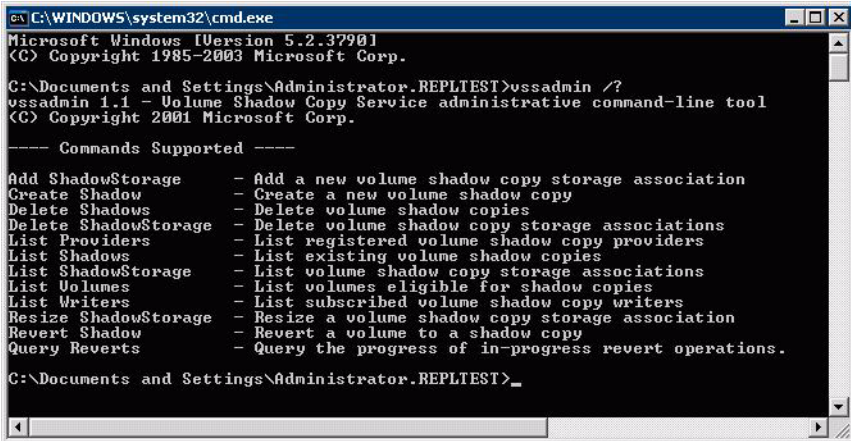Before creating Exchange shadow copies, you must install the Exchange Support utility.

RepliStor supports data replication from an MSCS cluster. If a node failure happens before the shadow copy is sent to the target, the shadow copy will not be created on the target. All future scheduled shadow copies will continue on the new node.

Allocating Shadow Storage

Prior to configuring any shadow copies, you will need to allocate shadow storage.

The vssadmin CLI is the interface to the Microsoft System Provider. This command line will be used to allocate storage for shadow copies and view the status of the Exchange writer when troubleshooting shadow copy creation problems.

In a DOS window type vssadmin /? for a list of commands. Refer to Figure 1.

Figure 1 Vssadmin command

It is important to be sure that sufficient shadow storage is being allocated on the target server as this is where the permanent shadow copies will be stored. The amount of storage necessary will vary depending on the size of the Exchange Storage Group(s), amount of data change during the retention period and the number of shadow copies which are being maintained before recycling.

Depending on the available resources, allocating multiple drives to increase performance and eliminate a single point of failure would be optimal.

Configuring Shadow Copies

If your system is running on a Windows 2003 platform, you can configure shadow copies for a specification via the **VSS Parameters** dialog box. This dialog box can be accessed in one of two ways:

◆ when you add a specification (select **Add Specification** from the **Maintenance** menu), the **VSS Parameters** dialog box displays after the **Options** dialog box.

◆ when you right-click a specification in the tree pane, select **Modify** and then click the **VSS Parameters** tab in the **Specifications** dialog box (Figure 2 on page 5).

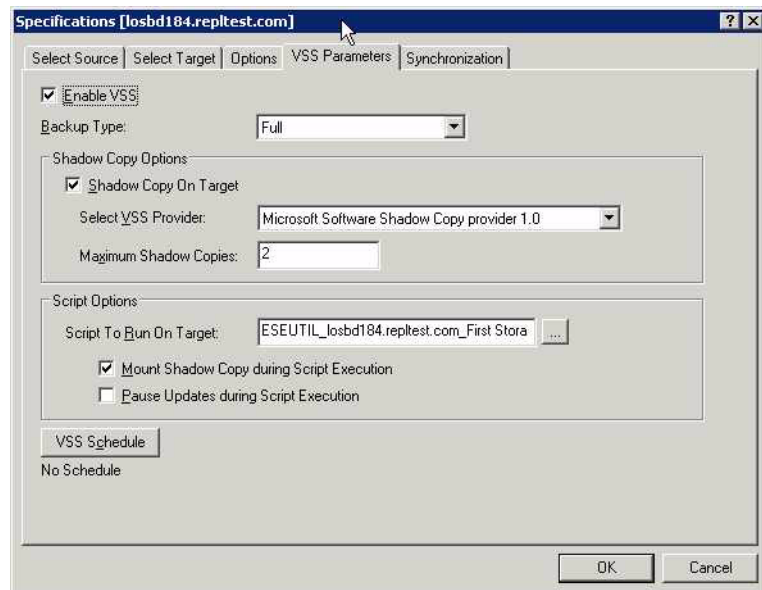

Figure 2   VSS Parameters Dialog Box

When the **Enable VSS** checkbox is enabled, Replistor takes a shadow copy of the drives associated with this specification. Enabling this option means you can request to take a shadow copy at any time on a particular specification.

The other parameters in the **VSS Parameters** dialog box are only relevant if the **Enable VSS** checkbox is enabled.

◆ **Backup Type** — This option specifies the type of shadow copy (backup type) that is performed on the source. This option is application/writer-dependent; in other words, it depends on what you want your specific application to do. For example, if you are taking a shadow copy of an Exchange database, and select **Full**, the log files will be truncated. If you are taking an Exchange shadow copy and selected **Copy** for the backup type, the log files would not be truncated. The backup types are the following:

   • **Full** — All files (regardless of whether they have been marked as backed up), are saved. Each file's backup history is updated to reflect that it was backed up.

   • **Copy** — Files are copied to a backup medium regardless of the state of each file's backup history, and the backup history is not updated.

◆ **Shadow Copy on Target** — Taking a target shadow copy is optional. The user may not require a shadow copy at the target and may instead run a script that for example, starts a backup or only copies files. When this option is checked, a *persistent* shadow copy is created on the target; the shadow copy will exist until you delete it.

◆ **Select VSS Provider** — The target system is contacted and a list of all VSS providers on that system is presented to the user. This option allows you to select the VSS provider to use when taking a shadow copy on the target such as CLARiiON® SnapView™ snapshots or Windows system shadow copies.

   RepliStor does not support reverting shadow copies made using the CLARiiON provider.

◆ **Maximum Shadow Copies** — This option determines the maximum number of shadow copies you want to keep on the target. Prior to creating the shadow copy on the target, old shadow copies are automatically deleted if the total number of shadow copy sets exceeds the user-defined maximum.

   For example, if you enter 5 maximum shadow copies, this means that RepliStor will delete all shadow copies on the target except for the last five. Before taking the target shadow copy, if this field is empty, it will never delete a shadow copy before taking another one.

◆ **Script To Run On Target** — This option allows you to select a script to run on the target after the shadow copy is created. For example, you can run the eseutil.exe utility on the target to make sure the target shadow copy is valid or a backup can be performed.

◆ **Mount Shadow Copy** — When this option is checked, the target shadow copy is mounted to a volume to become visible to the local host during execution of the script. It is unmounted when the script terminates. The following environment variables are set while executing the script: SHADOW_SET_PATH and SHADOW_SET_ID. The SHADOW_SET_PATH is set to the path where the shadow copy set has been mounted. SHADOW_SET_ID is the GUID of the shadow copy set.

◆ **Pause Update during Script Execution** — Updates are always paused during the target shadow copy operations to ensure that the shadow copy taken on the target is identical to the state of the source. Check this option if you need updates to remain paused during execution of the script. This option may also be used if no shadow copy was taken on the target and the script operation is relatively short.

◆ **VSS Schedule** — Click this button to schedule shadow copies for specifications. You can set a repeating schedule to take shadow copies by specifying a starting time and time interval (for example, minutes, hours, days, weeks, and so on).

Taking Shadow Copies

A shadow copy is associated with one or more specifications. Typically, a group specification is created that specifies all the related data. For example, a group specification may specify an Exchange Storage Group.

Important: If you are going to create a shadow copy of an Exchange Server 2003 database, before doing so, you must install the Exchange Support utility.

You can take a shadow copy of one specification or one group specification, or multiple specifications or group specifications by doing either of the following:

◆ right-click the specification(s) in the tree pane of the RepliStor client and select **Shadow Copy** (as shown in Figure 3 on page 8) or select the shadow copy button 📷 from the toolbar.

◆ manually issue the ShadowCopy CLI command.

Figure 3 **Taking a Shadow Copy**

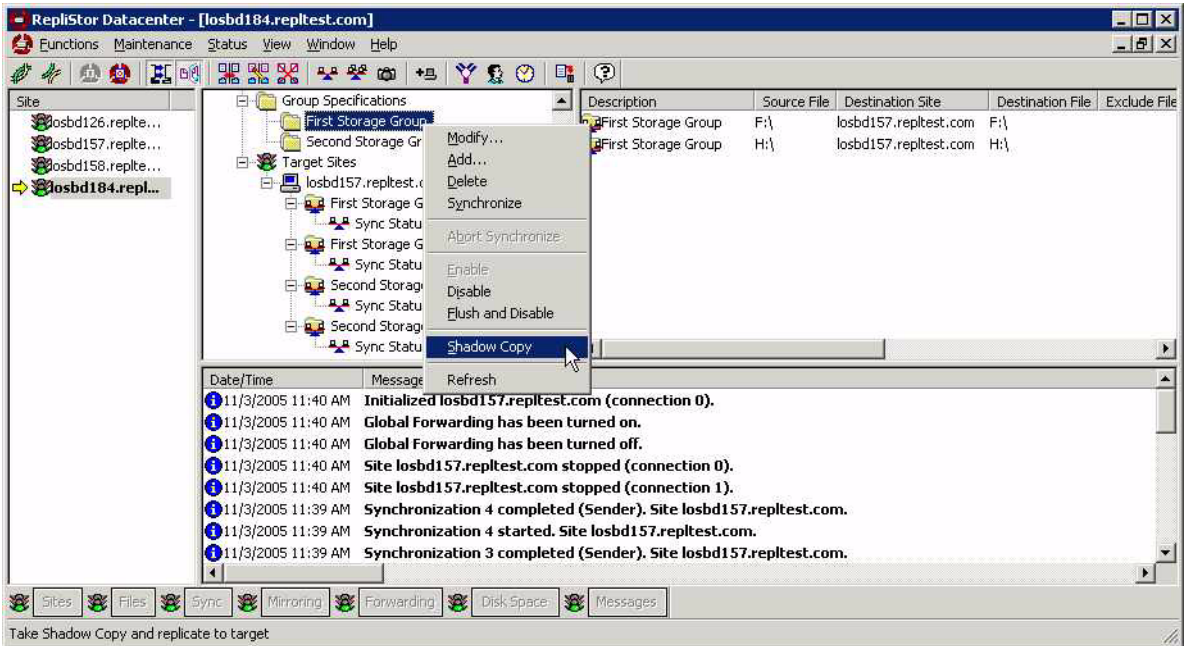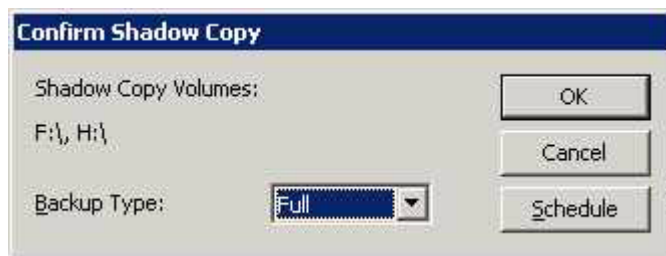After you select **Shadow Copy**, the confirmation message shown in Figure 4 appears.

Figure 4 **Shadow Copy Confirmation Dialog Box**

In the **Confirm Shadow Copy** dialog box, you can select the **Backup Type**. (refer to *Configuring Shadow Copies* on page 5 for more information on this option) and you can select the **Schedule** option to schedule shadow copies for specification(s).

Scheduling Shadow Copies

When you click **Schedule** in the confirmation dialog box shown in Figure 4, the **Shadow Copy Schedule** dialog box displays, as shown in Figure 5. You can set a repeating schedule to take shadow copies by specifying a starting time and repeat intervals (for example, minutes, hours, days) in the **Shadow Copy Schedule** dialog box.

When setting up shadow copy schedules, you cannot enter an end time or distinguish between weekdays and weekends. In addition, using the GUI, you cannot set two separate group specifications to shadow at the same time. If you want to set two separate group specifications to shadow simultaneously, you must use the CLI.

⚠ **CAUTION**

Microsoft Exchange routine maintenance performs a series of operations including defragmentation. Maintenance occurs by default between 1-5 am (configurable). It is highly recommended not to perform shadow copies during this period to avoid any additional overhead that may be caused by resource contention during this period.
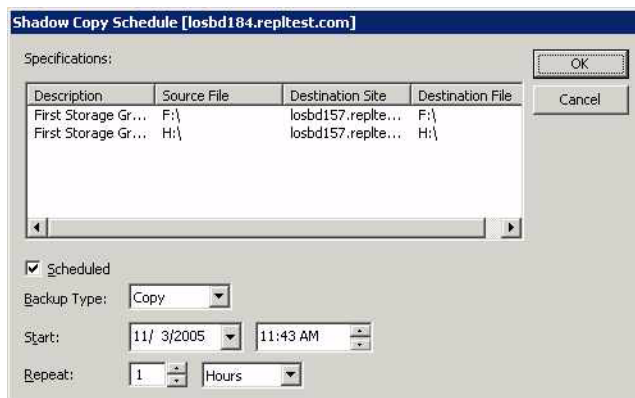
Figure 5   Scheduling Shadow Copies

After setting the shadow copy schedule (if desired), click **OK** in the **Shadow Copy Schedule** dialog box, and then click **OK** in the confirmation dialog box shown in Figure 4.

While the shadow copy is in progress, a **Shadow Copy** icon will appear in the upper part of the tree pane, and the Shadow Copy in Progress status will display in the right list pane, as shown in Figure 6.
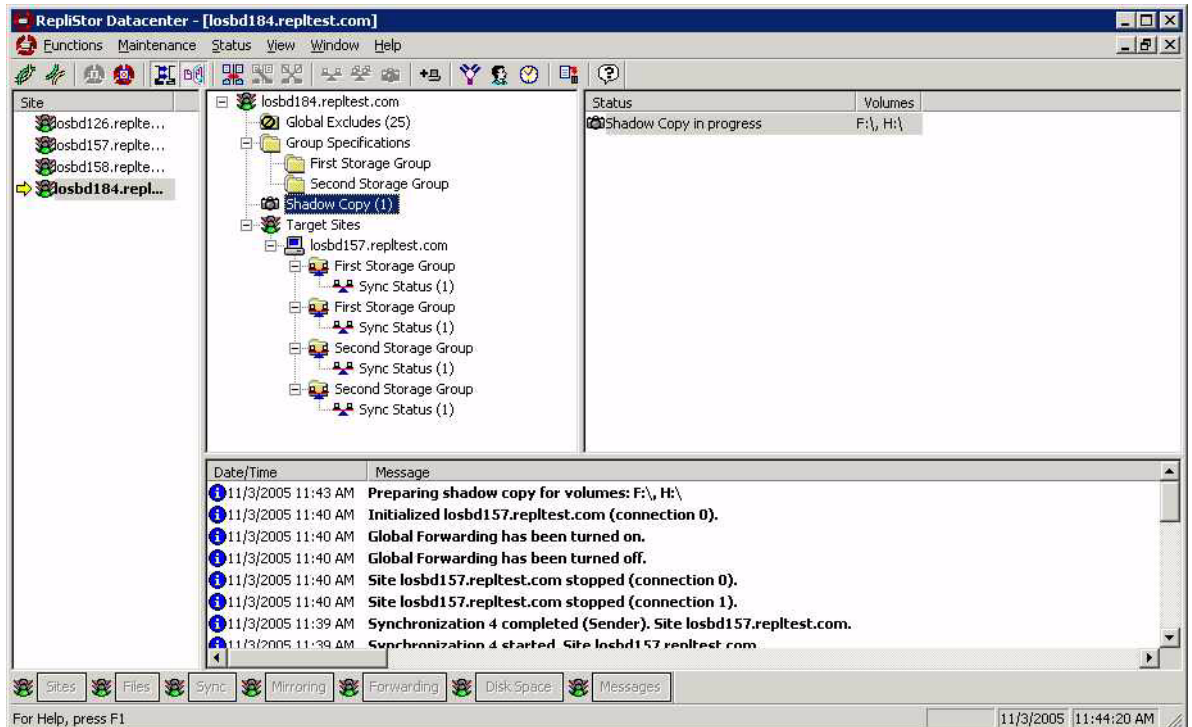

Figure 6   Shadow Copy in Progress

It is important to note that during the shadow copy process, a temporary shadow copy is created on the source system. Once a shadow copy is initiated, the source shadow copy shows up in the tree pane as the **Shadow Copy** icon, which is highlighted in gray in Figure 6. A source shadow copy has the following properties:

◆ It is not complete until the target shadow copy is complete and successful, and the target script (if any) has run and returns a SUCCESS error code.

◆ It is immediately marked *complete* if the target is not configured to take a shadow copy and there is no script to run.

◆ It is always marked as auto-delete and always uses the system VSS provider.

When the shadow copy has completed on the target, the target shadow copy set is designated by the **Shadow Copies Sets** icon 📷 in the tree pane, and the temporary source **Shadow Copy** icon disappears from the upper part of the tree pane, as shown in Figure 7. The target shadow copy sets are listed under the source site that they are associated with, but they reside on the target site.
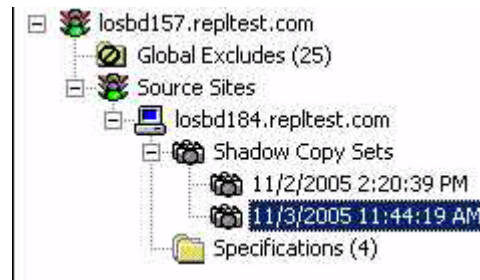
Figure 7   Shadow Copies Icon in the Tree Pane of the RepliStor Client Window

For more information on taking shadow copies, refer to Chapter 3 of the *EMC RepliStor for Microsoft Windows Version 6.1 Administrator's Guide*.

Microsoft Cluster Server (MSCS) Support

RepliStor supports data replication from an MSCS cluster. If a node failure happens before the shadow copy is sent to the target, the shadow copy will not be created on the target. All future scheduled shadow copies will continue on the new node, and any shadow copy schedules will also resume on the new node.

Managing Shadow Copies

Shadow copies are managed through the tree pane of the RepliStor client window, as shown in Figure 7.

To manage target shadow copy sets, you can either right-click the target shadow copy set in the tree pane or in the list pane. By right-clicking on a target shadow copy set, you can mount, unmount, delete, revert, or list the properties for a particular shadow copy set. Figure 8 on page 12 shows the target shadow copy right-click menu, and Table 1 on page 13 describes the right-click menu options.

Figure 8   Target Shadow Copy Right-click Menu

Table 1   Description of Target Shadow Copy Right-click Menu Options

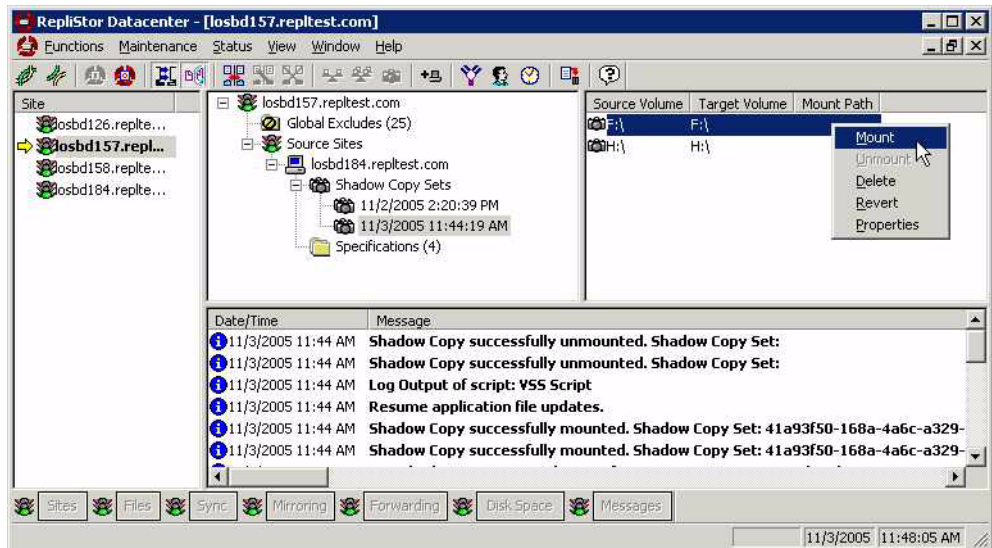| Right-Click Menu Option	Description
Mount	Mounts the selected shadow copy to an empty directory specified by the user.
Unmount	Unmounts the selected shadow copy from the directory.
Delete	Deletes the selected shadow copy.
Revert	Reverts the volume to the state of the selected shadow copy. The supported VSS providers for this option are the Microsoft system provider (if Windows 2003 SP1 is used) . VSS-compliant Service Pack 1 is required for the revert functionality. Microsoft recommends a hotfix, KB891957, that alleviates problems arising from depleted paged pool memory. Refer to KB 891957 on the Microsoft website, `http://support.microsoft.com`
Properties	Displays all the information known about this shadow copy. This should include: • Creation time • Shadow Copy set GUID • Shadow Copy GUID • Source server of the shadow copy • Source volume • Target volume • Mount path, if any • CLARiiON shadow copy information (if CLARiiON provider) • XML recovery document path

Canceling a Shadow Copy in Progress

You may want to cancel a shadow copy in progress, if for example, your target system becomes unavailable. In that case, the source system can not obtain the target shadow copy status and therefore it will never be marked Complete. You can cancel a shadow copy by right-clicking the shadow copy in progress in the right list pane and selecting **Cancel**, as shown in Figure 9 on page 14. When you cancel a shadow copy, a Warning log message is created indicating that the shadow copy was cancelled by the user.
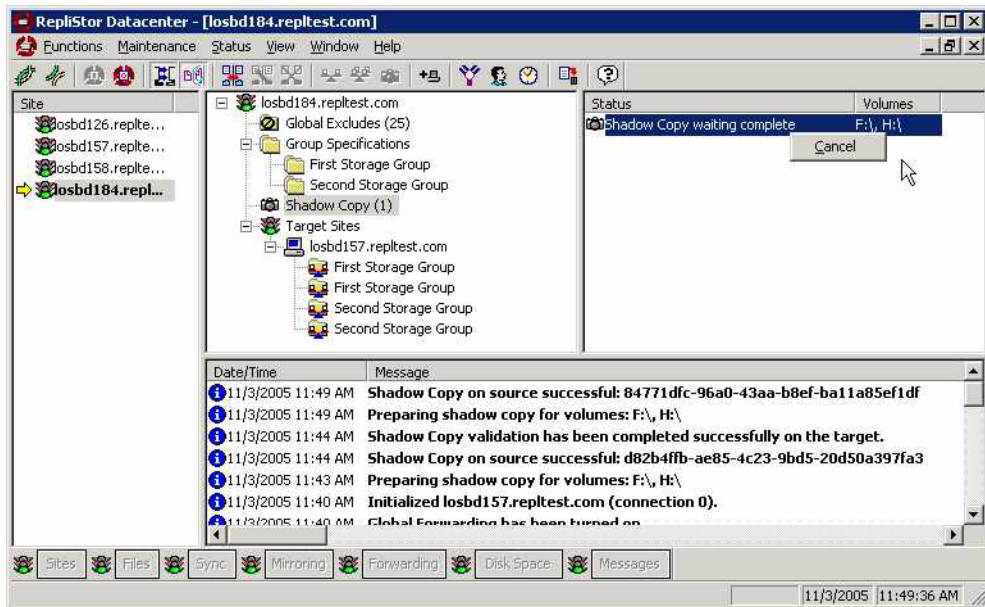
Figure 9   Cancelling a Shadow Copy in Progress

Simulation/Reporting

Overview   The simulation/reporting feature is a menu item you can select under **Maintenance** in the RepliStor console (Figure 10 on page 15). This feature allows you to simulate and report data bandwidth between the source and target systems. As shown in Figure 10, you can select a site in the left site pane, and then select **Maintenance**, **Simulation/Reporting** to monitor or simulate the traffic between the selected site and the target site. When you do this, the **Bandwidth Simulation/Reporting** dialog box appears (Figure 11 on page 16).
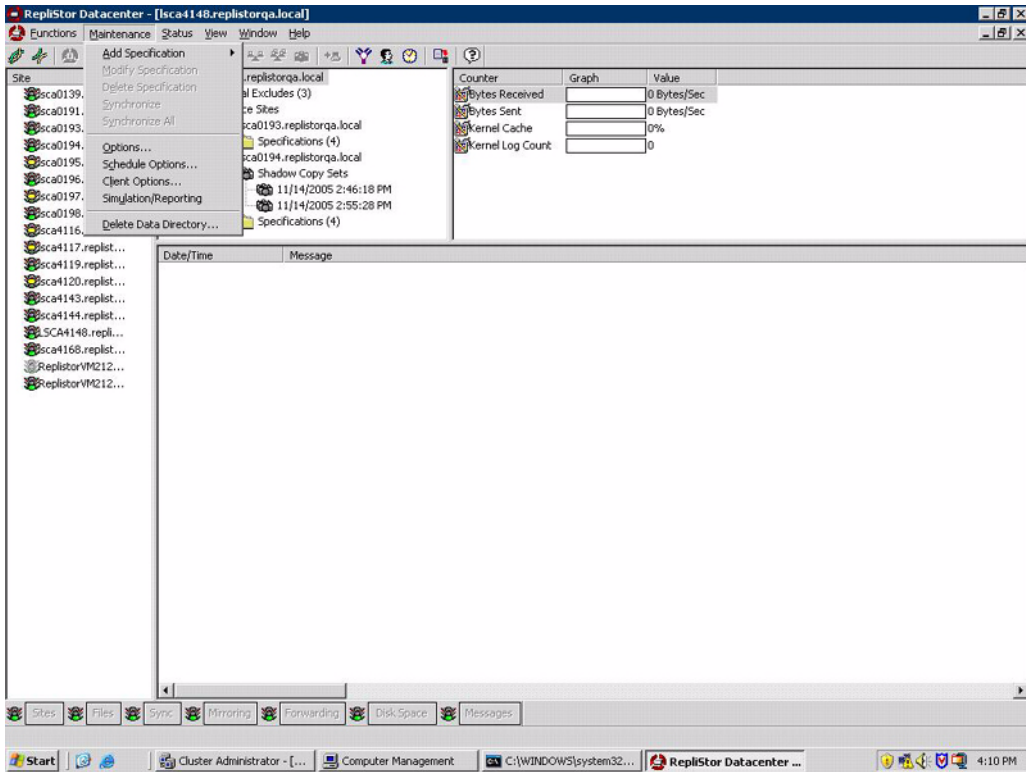
Figure 10   Simulation/Reporting Feature in Maintenance Menu
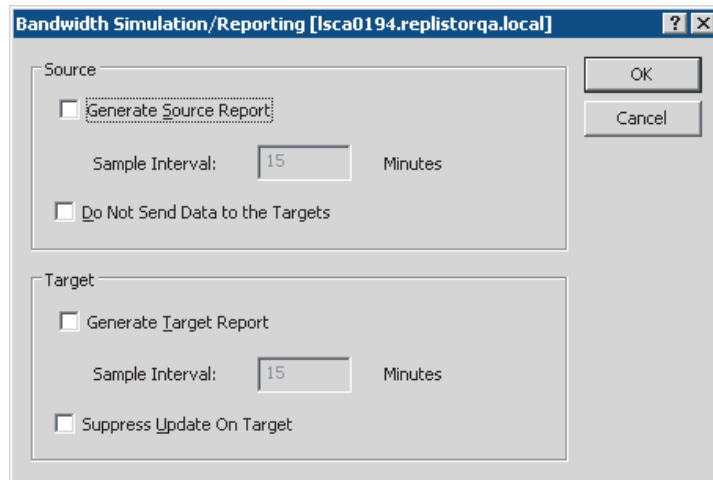
Figure 11   Bandwidth Simulation/Reporting Dialog Box

As shown in Figure 11 on page 16, you can configure simulation and/or reporting on either the source or the target. For example, you can report on the source system and suppress updates on the target system, and so on. It is important to note that the local RepliStor server can be either a source or a target.

Reporting   You can specify the sample interval in minutes at which you want to generate the source or target reports (for example, every 5 minutes, every 45 minutes, and so on). You can set the sample interval to generate source or target reports between 1 and 60 minutes. A smaller sample interval increases the accuracy of the bandwidth statistics between the source and the target at the expense of additional processing and larger file sizes.

The source and target reports are generated as text files in a comma-separated variable (csv) file format. Each row in the report is for a particular time period. The reports are stored in the Data directory.

An example of a source report is shown in Figure 12. The column headings displayed in the source report are described in Table 2 on page 17. The source report file name is of the form:
SourceReport.*year*.*month*.*day*.*hour*.*minute*.csv.

A target report example is shown in Figure 13 on page 18 and the target report column headings are described in Table 3 on page 19. The target report file name is of the form:

`TargetReport.`*`year.month.day.hour.minute`*`.csv`.

Time	Bytes Sent	Bandwidth Used, Bytes Sent	Kernel Cache Used	Kernel Cache High Water Mark	Kernel Cache Overflow Count	Kernel Cache Log Count	Kernel Cache Log Count High Water Mark	Number Open Files	rockn.studio.local-Replication Latency
5/17/2005 17:33	123583538	19460695	0	4	0	0	0	298	0
5/17/2005 17:38	140367733	21213232	0	4	0	0	0	455	0
5/17/2005 17:43	136496443	21328115	0	4	0	0	0	405	0
5/17/2005 17:48	123936886	19621642	0	4	0	0	0	379	0
5/17/2005 17:53	134563348	20634448	0	4	0	0	0	416	0
5/17/2005 17:58	134677879	20810912	0	4	0	0	0	520	0
5/17/2005 18:03	131217452	20464782	0	4	0	0	0	619	796
5/17/2005 18:08	123769775	19551314	0	4	0	0	0	330	0
5/17/2005 18:13	134535863	20508324	0	4	0	0	0	436	15
5/17/2005 18:18	142511724	22255441	0	4	0	0	0	558	15
5/17/2005 18:23	123858998	19637073	0	4	0	0	0	340	0
5/17/2005 18:28	139735546	21353282	0	4	0	0	0	491	0

Figure 12   Source Report Example

Table 2   Source Report Column Headings

Source Report Parameter	Description
Time	The date and time at which the source report was generated (in the example shown above in Figure 12, source reports were generated every five minutes).
Bytes Sent	The number of application data bytes sent from the source site to the target site since the last time the source report was generated. This number is cumulative in between intervals.
Bandwidth Used, Bytes Sent	The number of application data bytes sent from the source site to the target site, after any compression, since the last sample time. This number is cumulative in between intervals and represents the actual amount of data sent on the network.
Kernel Cache Used	The percent of the kernel cache used by the source site in sending data to the target. The kernel cache is a fixed amount of shared memory used for queuing data going from the source to the target.
Kernel Cache High Water Mark	The highest percent the kernel cache has used since the last time it overflowed and was reset.
Kernel Cache Overflow Count	The number of times the kernel cache has overflowed and began using `OC$` files.

Table 2   Source Report Column Headings (continued)

Source Report Parameter	Description
Kernel Cache Log Count	The number of `OC$nnnnn.rdf` files that are currently in the data directory. Each log holds approximately 1 MB of data by default.
Kernel Cache Log Count High Water Mark	The highest number of `OC$nnnnn.rdf` files that had existed.
Number Open Files	The number of open files that the RepliStor kernel driver is currently tracking.
<target> - Replication Latency	The number of milliseconds that it currently takes between the time the application performs the file operation and when that file operation is performed on the target. This column displays for every current target site.

Time	Bytes Received	Bandwidth Used, Bytes Received	photo.studio.local:0-Target Queue
5/17/2005 17:36	306668	306668	0
5/17/2005 17:41	306964	306964	0
5/17/2005 17:46	303100	303100	0
5/17/2005 17:51	303268	303268	0
5/17/2005 17:56	303212	303212	0
5/17/2005 18:01	303520	303520	0
5/17/2005 18:06	303100	303100	0
5/17/2005 18:11	303100	303100	0
5/17/2005 18:16	303212	303212	0
5/17/2005 18:21	303744	303744	0
5/17/2005 18:26	303044	303044	0
5/17/2005 18:31	303044	303044	0
5/17/2005 18:36	303800	303800	0
5/17/2005 18:41	303156	303156	0
5/17/2005 18:46	308756	308756	0

Figure 13   Target Report Example

Table 3	Target Report Column Headings

Target Report Parameter	Description
Time	The date and time at which the target report was generated (in the example shown above in Figure 13, target reports were generated every five minutes).
Bytes Received	The number of application data bytes received by the target site since the last sample interval. This number is cumulative in between intervals.
Bandwidth Used, Bytes Received	The number of application data bytes received by the target site, after any compression, since the last sample time. This number is cumulative in between intervals and represents the actual amount of data received on the network.
<source>:*<connection ID>* - Target Queue	Size of the target queue at the sample interval. This value, by default, should never exceed 100. If it is varying between 50 and 100, this indicates that there is a bottleneck on the target side in updating the disk, and it is slowing down the source system from sending data.

Simulation RepliStor allows you to simulate data replication where data is not actually sent to the target system. If used in conjunction with the reporting function, the simulation function is useful for determining the volume of data that is to be replicated as well as peak activity times, without loading the network or having a target system capable of handling the data from the source.

If you don't want to use real data for the source configuration, you can simulate the source bandwidth by selecting the **Do Not Send Data to the Targets** checkbox as shown in Figure 11 on page 16. Selecting this option will prevent the source from sending data to the targets. If this option is selected, any data that is to be sent to the targets will be lost. If the **Do Not Send Data to the Targets** checkbox is not selected, the data is sent to the target (this is the default).

For the target configuration, selecting the **Suppress Update on Target** checkbox means that the local RepliStor server will not be updated with incoming data (that is, any data received from the source system will be ignored). All incoming data will be lost. This option is recommended if you want to run a simulation where the target system does not have the disk capacity to handle all of the source data. If the **Suppress Update on Target** checkbox is not selected, then data will be written to the local server.

When you select the desired options in the **Bandwidth Simulation/Reporting** dialog box, click **OK**.

If a report is in progress, you will see a **Reporting in Progress** message in the status bar in the lower right corner of the RepliStor client, as shown in Figure 14 on page 20.

If a simulation is in progress (that is, if you selected either or both of the **Do Not Send Data to the Targets** or the **Suppress Update On Target** options), you will see a **Simulation in Progress** message in the lower right corner of the RepliStor client. This message displays to remind you that a simulation is running, as this is easy to forget once you set up the simulation.
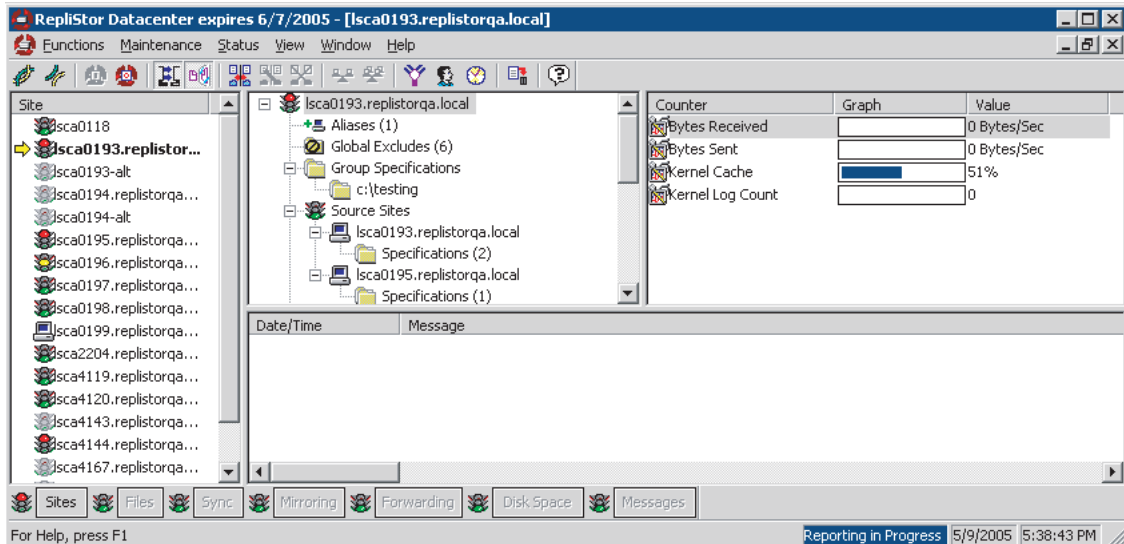

Figure 14   Reporting in Progress Message in Lower Right Status Bar

Mount Points Supported on Source

RepliStor Version 6.1 now supports mount points on the source system. RepliStor can replicate data in specifications that span mount points. It will also automatically take shadow copies of all mounted volumes within a specification.

For mount point limitations, refer to *Mount Point Limitations* on page 28.

Fixed Problems

Table 4 displays problems that have been fixed in RepliStor Version 6.1.

Table 4   Fixed Problems

Bug ID	Description
LGTpa63938	Add warning when two sources mirror to the same target path.
LGTpa68348	Invalid Target typed in, use tab, you are left in the wrong field.
LGTpa69118	Receiver thread cannot determine IP address of source computer.
LGTpa73171	Email for remove alias from target is missing.
LGTpa73632	Renaming an excluded folder does not work correctly.
LGTpa73818	Failback after automatic failover - DNS removal error.
LGTpa74047	Replistor continuous refresh on startup for user with View Status permission removed.
LGTpa74178	Popups display for unattached machines in the site pane.
LGTpa74238	The Exchange Installer Support program should accept the host machine as the target.
LGTpa74262	SPN is not added when machine is not in Active Directory.
LGTpa74268	SPN setting is not used unless alias is deactivated/activated.
LGTpa74581	On 64-bit systems, file is written as uncompressed, but mirrored compressed.
LGTpa76431	When starting client, many popup errors display.
LGTpa76786	If Auto Start service is unchecked, dim **Boot Load Driver**.
LGTpa76871	Warning message: cannot change thread mode after it is set.
LGTpa77220	Validation tests failing on 64 bit - archive bit.
LGTpa77255	GUI changes for source server.
LGTpa77257	Source and Target path are not same.
LGTpa77394	SPN for Alias is not added on target.
LGTpa77414	Disk Monitor default settings must be updated.
LGTpa77415	Site Forwarding schedule and throttling options not saved when you upgrade from version 5.3.4.

Table 4   Fixed Problems (continued)

Bug ID	Description
LGTpa77877	Restored support for `nocircular` command.
LGTpa78070	Handling Improper Inputs in the **Advanced** tab of the **Options** dialog box (**Maintenance**, **Options**, **Advanced**).
LGTpa78457	Modify the `exch2k.dll` operations vis-a-vis the RUS.
LGTpa78511	Blocked file test - file writes are done out of order.
LGTpa79062	OS version check is not made with silent install.
LGTpa79445	Disk Space Monitor may monitor wrong partition (if mount point).

Environment and System Requirements

This section discusses the system requirements the source and target servers must meet in order to run RepliStor software.

Before installing RepliStor software, you must have administrative privileges on the system where you are installing the product. If you are installing in a domain, the account must be in the Domain Admins group. You can install RepliStor software over a network if you have administrative privileges on both the source and target machines.

Operating System and Server Requirements

Before installing RepliStor software, you must meet the following operating system and server requirements:

◆ Operating systems:

- Windows 2000 (Service Pack 4 is recommended)
- Windows Server 2003
- Windows Server 2003 64-bit Itanium Edition
- Windows Server 2003 64-bit x64 Edition (AMD Opteron and Intel EM64T)
- Windows Powered Network-Attached Storage (NAS) 2000
- Windows Storage Server 2003
- Windows XP Service Pack 2

The VSS-compliant shadow copy functionality is only supported on Windows 2003 systems.

◆ Server hardware certified by Microsoft for the version of Windows that you are running

For a list of servers certified by Microsoft, refer to the Microsoft Windows Compatible Products page on the Microsoft website at `http://www.microsoft.com/windows/compatible/`, or contact a Legato® Sales Representative.

Software Requirements

RepliStor -- Windows Installer 2.0 or later is required. If your system has an earlier version, you must obtain Windows Installer 2.0 or later from the Microsoft website. Windows 2000 Service Pack 4 and later includes the Windows Installer 2.0 standard.

DiskXtender 2000 -- Version 5.60.049 patch 4 or later is required.

Communication Requirements

RepliStor software supports the TCP/IP protocol. The Windows systems you use must be able to communicate with each other. To verify communication, use File Manager or Windows Explorer to establish a network connection from one machine to another.

Disk Space Requirements

The information in this section should be considered as guidelines only. These recommendations depend on several variables. For example, the amount of storage on the source and target may be significantly greater if you are replicating data that changes quickly or if the links are relatively slow. In addition, if you are using scheduled forwarding or throttling you may actually need more space than the original amount replicated. This scenario could occur if you accumulate changes all day, and then turn forwarding back on at night. Take your data storage needs into consideration before choosing a reserve size.

EMC recommends the following disk space for program, documentation, and log files:

◆ **Program files** — The following platforms require the disk space shown for program files:

- Intel 32-bit version: 18 MB

- Itanium (ia64): 36 MB

- Opteron (x64): 27 MB

◆ **Log files** — Allocate space for the following types of log files:

- **Kernel cache** — The kernel cache is a fixed amount of shared memory used for queuing data going from the source to the target. When you install the RepliStor software, it looks at the physical memory and preconfigures an appropriate setting for

the system. The kernel cache size defaults to 5 percent of physical memory. However, you can modify this parameter, if needed, in the RepliStor **Options** dialog box (on the **Advanced** tab).

It is important to size this memory segment correctly. If it is too small, output from memory operations may overflow to disk (that is, OC$nnnnn files in the RepliStor data directory), hurting performance. If the memory segment is too large, it reduces the amount of memory available to other applications.

For information on how to size the kernel cache appropriately, refer to the *Sizing the Kernel Cache* on page 5-3 of the *EMC RepliStor for Microsoft Windows Version 6.1 Administrator's Guide*.

- **Message log** — The message log holds 1,000 messages by default; it typically requires approximately 3 MB.

- **Blocked files (target only)** — The blocked files log holds all the file operations that are queued to all blocked files. This file can grow to any size depending on what is in queue.

- **OC$nnnnn files (source only)** — The OC$nnnnn log holds all the file operations that are queued to be sent to the target if the kernel cache overflows. The most common reason the kernel cache overflows is when a target site is blocked and the file operations cannot be forwarded.

RepliStor Software Use of Windows Active Directory

When installing RepliStor software, you can optionally register it in Active Directory. This has the following benefits:

- There is a common site list for all RepliStor installations in the domain. If any server makes a change to the site list, *all* servers see that change immediately.

- There is a common users list for all installations in the domain (on the **Users** tab in the **Options** dialog box).

- The site list is available immediately. Manually adding a site is only necessary if the site is outside the domain.

In order to register RepliStor software in Active Directory, the user performing the installation must be in the Domain Admins group. Once RepliStor software is installed, a domain administrator can assign administrative rights to any other user or group.

RepliStor software uses the base Active Directory schema and does not extend the schema. The only portion of Active Directory that RepliStor software modifies is:

DC=domain

    CN=System

        CN=Legato

            CN=RepliStor

Under the RepliStor entry is an entry for each installed RepliStor server, as well as entries for each external RepliStor server (as added into the Site List). Use the following information to determine the additional disk space the system requires to replicate RepliStor Active Directory updates:

◆ Each RepliStor installation typically requires less than 1 KB of additional space in Active Directory, although this depends on the number of characters entered in the text fields in the **Site Properties** dialog box (for example, **Description**, **Site Name**, **Account**, **Password**).

◆ All attributes that RepliStor software uses in Active Directory are sent during both full and partial Active Directory replications.

◆ RepliStor Active Directory updates are confined to user-initiated events, such as installing and removing RepliStor software, and modifying site properties.

Compatibility with Other Releases of RepliStor Software

RepliStor Version 6.1 is compatible with Versions 4.0, 4.1, 4.2, 5.0, 5.1, 5.2, 5.3, and 6.0; however, you will not be able to modify information under the **Users** tab of the **Options** dialog box in earlier versions. In addition, if you are running version 4.2 or later with aliases defined for Super Automatic Switchover (Super ASO), all systems must be running RepliStor Version 4.2 or later.

Known Problems and Limitations

This section contains the known problems and limitations in RepliStor Version 6.1.

Known Problems

Table 5 displays known problems in RepliStor 6.1.

Table 5   Known Problems

Bug ID	Description	Workaround
LGTpa75301	When an administrative installation is done, the `msi` file created is `rep60422c.msi`. This is fine UNLESS you are doing a remote installation. Remote installations fail because the `msi` file is incorrect	After performing an administrative install, in the new directory you created during the administrative install, rename the msi file to `replistor.msi`.

Limitations

The following limitations exist in RepliStor Version 6.1.

RepliStor and MSCS Clusters

Consult the note below before installing RepliStor or upgrading RepliStor in Microsoft clusters.

⚠️ **CAUTION**

When installing RepliStor into a Microsoft cluster, it must be installed in the same directory path on each node. If all nodes are not installed on the same path, Cluster Server may not be able to use RepliStor resources on all nodes.
In addition, when upgrading RepliStor installations that are in a Microsoft cluster to RepliStor Version 6.1, all nodes must be upgraded to Version 6.1; otherwise the RepliStor resources may not be functional on one or more nodes.

Kernel Stack Space Considerations

On Windows 2000 systems, a blue screen may occur due to stack overflow errors in the kernel space. This may happen if many kernel drivers are loaded. While a single driver alone may not overflow the stack, all of them together may result in an overflow error message similar to the following:

```
STOP 0x0000007F (0x00000008, 0x00000000, 0x00000000,
   0x00000000)
(UNEXPECTED_KERNEL_MODE_TRAP)
```

Microsoft has released a hot fix for Windows 2000 that addresses this problem by allowing drivers to conserve stack space. Until now, only Windows XP and Windows 2003 platforms had this functionality.

RepliStor Version 6.1 will detect whether this hot fix has been installed on Windows 2000. If it has been installed, RepliStor Version 6.1 will utilize this new functionality to conserve stack space and blue screens should not occur.

This hot fix will be included in Windows 2000 Service Pack 5. If you are receiving blue screen errors now, download the hot fix according to Microsoft Knowledge Base Article 835281 available at:
`http://support.microsoft.com/?kbid=835281`

Mount Point Limitations

◆ Global Excludes will not work if it spans a mount point. In other words, if you have a global exclude, such as: "`e:\*.doc`" with the Subdirectories flag set, it will exclude replication of all `*.doc` files on all subdirectories unless that file is in a mounted volume under `e:\`. In that case, that global exclude is not in effect.

◆ Protect Target Files function will not work if the target files span a mount point. All files under the mount point will not be protected.

Technical Notes

This section discusses reboot scenarios and DiskXtender requirements for RepliStor.

Rebooting Issues When Installing, Upgrading, or Uninstalling RepliStor

RepliStor uses a file system filter driver. Because of a Windows limitation, a reboot is required to stop a filter driver in order for it to be upgraded or uninstalled. This is a Windows limitation, not a RepliStor limitation. Windows allows drivers to be installed and started, but you cannot stop a filter driver without risking a blue screen.

Microsoft has introduced a new framework for filter drivers called Filter Manager. Using the Filter Manager, it is now possible to stop a driver. This means that an upgrade or uninstall can be performed without a reboot. RepliStor Version 6.0.x supports the Filter Manager, but RepliStor can only use the Filter Manager if it exists in the operating system on which RepliStor is being installed on. At the time of this writing, the systems that include Filter Manager are Windows XP SP2, Server 2003 SP1, and Windows 2000 SP4 with Update Rollup 1. For all upgrades or uninstalls for RepliStor Version 5.3 and earlier, a reboot will be required even if the system being installed does have the Filter Manager.

Upgrading/Uninstalling RepliStor 6.0.x on Windows Server 2003 SP1 or Later Systems

An upgrade or uninstall of a RepliStor 6.0.x build on a Windows Server 2003 SP1 or later system will not require a reboot.

Installing RepliStor 6.0.x on Windows XP SP2 or 2000 SP4 with Update Rollup 1 Systems

If installing RepliStor *for the first time* on either a Windows XP SP2 system, or a Windows 2000 SP4 with Update Rollup 1 system, RepliStor will take advantage of the Filter Manager that exists on these operating systems.

However, in order to minimize any potential Filter Manager impacts, Microsoft has set the Filter Manager to be inactive unless it is used. When RepliStor attaches to it, the Filter Manager is activated, but since it was not activated at boot time, there are two potential problems:

◆ The RepliStor driver may not be layered correctly with other drivers.

◆ There may be an intermittent problem with the Filter Manager that causes it to not attach to certain volumes.

Configuring the Filter Manager to start at boot time fixes both of these problems, but requires a reboot. Therefore, after installing RepliStor for the first time on Windows XP SP2 or Windows 2000 SP4 with Update Rollup 1 systems you must reboot. After the this initial reboot, you can upgrade, install, or uninstall RepliStor without any further reboots.

This issue does not exist with Windows Server 2003 or later versions of the operating system, since the Filter Manager is active by default.

Installing RepliStor 6.0.x on Windows 2000 SP4 (without Update Rollup 1) or Earlier Systems with SNMP Functionality

If you are installing RepliStor and require SNMP functionality and you are installing on a Windows 2000 SP4 or earlier system (without Update Rollup 1), you must manually reboot so that the SNMP service can attach to the RepliStor SNMP extension agent. If you do not reboot after installing RepliStor, you will notice an error in the Event Viewer similar to the following example:

```
Event Type: Warning
Event Source: SNMP
Event Category: None
Event ID: 1102
Date: 8/31/2005
Time: 9:32:28 AM
User: N/A
Computer: VPC1
Description:
The SNMP Service is ignoring extension agent dll
C:\Program Files\Legato RepliStor\SNMPAGNT.DLL
because it is missing or misconfigured.
Data:
0000: 7e 00 00 00 ~...
```

A reboot will resolve the above error.

If running Windows 2000 SP4 with Update Rollup 1, or any later operating system version (Windows XP, 2003, and so on), a reboot is not necessary.

DiskXtender Requirements

If you are using DiskXtender 2000 with RepliStor Version 6.0.x, you must use DiskXtender Version 5.60.049 patch 4 or later

Best Practices When Using Shadow Copies

When using shadow copies, take note of the following:

◆ If a volume is configured for shadow copies it should NOT also be used for shadow storage.

◆ Shadow storage must be spread between multiple volumes to prevent problems reverting multiple volumes at once.

◆ Standard behavior for the Microsoft system provider is that when a shadow copy is reverted all newer shadow copy sets for that volume are deleted

Documentation

The following documents, available on the EMC Legato website at www.legato.com, provide additional information about the RepliStor software:

◆ *EMC RepliStor for Microsoft Windows Version 6.1 Administrator's Guide,* P/N 300-002-464 Rev A01

◆ *EMC RepliStor for Microsoft Windows Version 6.1 Installation Guide,* P/N 300-002-227-463 Rev A01

◆ EMC RepliStor online help system

If your environment includes other vendors' storage systems, refer to the appropriate documentation from your vendor.

Software Media, Organization, and Files

The EMC RepliStor for Microsoft WindowsVersion 6.1 kit consists of this document and the following:

◆ EMC RepliStor for Microsoft WindowsVersion 6.1 CD

◆ *EMC RepliStor for Microsoft Windows Version 6.1 Administrator's Guide,* P/N 300-002-464 Rev A01

◆ *EMC RepliStor for Microsoft Windows Version 6.1 Installation Guide,* P/N 300-002-463 Rev A01

Installation

This section describes how to install, upgrade, and remove RepliStor Version 6.1 software.

Before You Install

Be aware that RepliStor software must be installed as a service that runs under the System account or an authenticated account in the Administrators group (or Domain Admins, if installed in a domain). It cannot run under a user's account because of Windows operating system limitations. Specifically, RepliStor software needs to communicate with the RepliStor kernel mode driver. Only System or Administrator users are allowed to perform this function.

For information on securing remote servers, refer to *Setting Up Secure Access to Remote Servers* on page 1-13 of the *EMC RepliStor for Microsoft Windows Version 6.1 Installation Guide.*

During installation, RepliStor software prompts you for the following information:

◆ The pathname to install RepliStor programs. The recommended path is:

```
%SystemDrive%\Program Files\Legato RepliStor
```

◆ The pathname to store RepliStor data and script files. The default paths to data and script files are:

```
%SystemDrive%\Documents and Settings\
   All Users\Application Data\Legato RepliStor Data
```

and

```
%SystemDrive%\Documents and Settings\
   All Users\Application Data\Legato RepliStor Scripts
```

To change the program directories after installing RepliStor software, you must reinstall it. To change the location of the data directory after installing RepliStor software, you must change it on the **Directories** tab in the **Options** dialog box (select **Options** from the Maintenance menu).

Obtaining a License Key

When you first install RepliStor software, you can select **Request Evaluation License** for a trial version. Before you install a non-evaluation copy of RepliStor, however, you must obtain a license key from Legato for each computer on which the product will run. When you obtain a license key, you automatically register the software and activate support for RepliStor software.

If you are installing RepliStor from a CD-ROM, you must contact Legato and give them the serial number listed on the software package to obtain a license key.

For additional information, refer to *Obtaining a License Key* on page 1-7 in the *EMC RepliStor for Microsoft Windows Version 6.1 Installation Guide.*

Microsoft Windows Storage Server Support

RepliStor Version 6.1 supports Microsoft Windows Powered Network-Attached Storage (NAS), including Windows Storage Server 2003. Built on the Windows Server 2003 operating system, Windows Storage Server 2003 is a dedicated file and print server that supports heterogeneous file serving, as well as backup and replication of stored data. For information about obtaining a license key to run RepliStor on Windows Storage Server, refer to *Obtaining a License Key* above.

To install RepliStor software on a system running Windows Powered NAS, you must use Terminal Services or Remote Desktop. For information about these features, refer to the Microsoft Windows documentation.

Installing RepliStor Software

This section provides instructions for installing RepliStor software from a CD-ROM, a single file web distribution, and from the msiexec command.

How to Install RepliStor Software from a CD-ROM

To install RepliStor software from a CD-ROM:

1. Start Windows.

   The user ID to log on to Windows must have administrative privileges, or Domain Admins if you are installing in a domain.

2. Insert the RepliStor CD-ROM into the CD-ROM drive. If the RepliStor Setup Wizard doesn't start automatically, click the RepliStor.msi file.

3. Follow the prompts in the Windows Installer program to install the program.

How to Install RepliStor Software from a Single File Web Distribution

You can install RepliStor software from a single file obtained from the web. If you obtain RepliStor software over the Internet, it is packaged as a single, compressed file named rep<vvbbb>.msi, where vvbbb is the version and build number. To install the RepliStor software, you execute the file and follow the RepliStor Setup Wizard prompts.

How to Install RepliStor Software Using the msiexec Command

Use the msiexec command with the replistor.msi installer database to specify non-standard options, uninstall the RepliStor software, or perform an administrative install.

Example: Using the msiexec Command

The following example shows the command and parameters to enter for an unattended installation that allows you to view the installation's progress, and cancel and override the default installation and data directories. (Note that the command wraps in the example, but should be entered on a single line.) Once you are in the folder that contains the setup.exe file, type:

```
msiexec /i replistor.msi /qb INSTALLDIR="f:\Legato
   RepliStor" DATADIR="f:\RepliStor Data"
```

The following example shows how to specify an administrative installation:

```
msiexec /a replistor.msi
```

For more information on using the msiexec command to install RepliStor software, refer to *How to Install RepliStor Software Using the msiexec Command* on page 1-8 in the *EMC RepliStor for Microsoft Windows Version 6.1 Installation Guide*.

Windows XP Considerations

RepliStor Version 6.1 supports Microsoft Windows XP SP2. When you are installing RepliStor on a system running Windows XP, RepliStor is automatically registered as an application for the firewall. When you use the RepliStor Setup Wizard to install RepliStor on a Windows XP system, there is a **Register RepliStor with the Windows Firewall** checkbox that is checked by default at the bottom of the **Replistor Parameters** dialog box. If you leave this box checked, the RepliStor service and the RepliStor control service are automatically registered with the firewall.

Verifying RepliStor Software Installation

Select **Start**, **Programs**, **RepliStor** from the Windows desktop to start the product and verify that it has installed correctly.

Upgrading RepliStor Software

This section describes how to upgrade EMC Legato RepliStor, Versions 5.0, 5.1, 5.2, 5.3, and 6.0 for Microsoft Windows.

The RepliStor Version 6.1 installation program determines if Versions 5.0, 5.1, 5.2, or 5.3 reside on the system before installing. If any of these versions are running, the setup program prompts you to reboot the system during installation. Installation will resume after the system reboots.

You need a new license key when upgrading from a previous RepliStor version (other than Version 6.0) to RepliStor Version 6.1.

Removing RepliStor Software

To completely remove all RepliStor executables, data files, and Windows Registry entries from a target or source system:

1. From the **Windows Control Panel**, double-click **Add/Remove Programs**.

2. From the list of programs, select RepliStor, and then click **Remove**.

3. Follow the **Uninstall** dialog prompts.

4. If RepliStor software was run since the last system boot, you are prompted to reboot to complete the uninstall.

The RepliStor Scripts directory is not removed if it is not empty. Any files added to the data directory after installation are not removed (for example, log files).

Troubleshooting and Getting Help

This section provides specific and non-specific troubleshooting information.

Troubleshooting Shadow Copy Creation

Exchange shadow copy creation failures are logged in both the RepliStor message logs and the Application Event Log. Microsoft logs all application specific information in the Event Log which consists of the Application Event log and the System log. Thus, any given message may be logged in either the Application Event log or the System log.

When troubleshooting shadow copy creation, consider the following:

◆ Check the repliStor messages log. To see RepliStor messages in the message pane, right click and enable Info, optionally Debug messages can enabled.

◆ To enable debug messages edit the following registry key and set the value to 1:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
    RepliStorControl\Parameters\Enable Debug Log
```

◆ After setting the key, restart the RepliStor server and control services.

In addition to the logs, querying the status of the writer can also determine its current state. For example the writer may not have been properly started or a backup may have been in progress. If the event log is backed up, the VSS admin commands can give better results.

◆ Issue the following command from a DOS window to view the state (refer to Figure 1-1):

Vssadmin list writers

Figure 1-1   Vssadmin list writers command

If any error is returned, restart the Volume Shadow Copy Service and the Exchange Information Store Service from the Services Applet to reset the writer state.

General Help

For questions about technical support, contact EMC Customer Support at:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

Follow the voice menu prompts to open a service call and select the applicable product support.

For the list of EMC sales locations, access the EMC home page at:

http://www.emc.com/contact/

For additional information on EMC products and services available to customers and partners, refer to the EMC Powerlink™ website at:

http://powerlink.emc.com