

Open Systems SnapVault® 2.1.1 Release Notes

Release notes contents

These release notes contain the following topics:

- ◆ [What you can do with Open Systems SnapVault](#)
- ◆ [What is new with Open Systems SnapVault 2.1.1](#)
 - ❖ [Primary fix in Open Systems SnapVault 2.1.1](#)
 - ❖ [All issues fixed in Open Systems SnapVault 2.1.1](#)
- ◆ [What is new with Open Systems SnapVault 2.1](#)
 - ❖ [New features](#)
- ◆ [Preinstallation considerations](#)
 - ❖ [System requirements for the Open Systems SnapVault agent](#)
 - ❖ [Issues and limitations](#)
 - ❖ [Where to find status and problem reports](#)
 - ❖ [Fixed issues in Open Systems SnapVault 2.1](#)
 - ❖ [Known issues in Open Systems SnapVault 2.1](#)
 - ❖ [Central management of Open Systems SnapVault agents](#)
- ◆ [Details of the Open Systems SnapVault 2.1 agent features](#)
 - ❖ [Backup and restore of Windows System State data](#)
 - ❖ [Backup exclusion lists](#)
 - ❖ [Checkpoint restart support of update transfers](#)
 - ❖ [EFS encrypted file backup and restore](#)
 - ❖ [Block-level incremental backup](#)
 - ❖ [BLI backup of certain name-based files](#)
 - ❖ [Windows NT and Windows 2000 OFM option](#)
 - ❖ [Windows 2003 VSS snapshots](#)
 - ❖ [SnapVault secondary protection using SnapMirror](#)
 - ❖ [Checkpoint restart of initial transfers](#)
 - ❖ [The snapvault command on the primary storage system](#)
- ◆ [Installing Open Systems SnapVault agents on Windows platforms](#)
 - ❖ [Installing a Windows agent from CD-ROM](#)
 - ❖ [Installing a Windows agent from NOW](#)
 - ❖ [Using the Installation Wizard](#)
 - ❖ [Remote batch installation of the Open Systems SnapVault agent on Windows](#)

- ◆ Installing Open Systems SnapVault agents on Solaris, HP-UX, AIX, IRIX, or Linux platforms
 - ❖ Installing the Solaris agent from CD-ROM
 - ❖ Installing the Solaris agent from NOW
 - ❖ Using the Solaris pkgadd utility to install the Solaris agent
 - ❖ Installing the HP-UX, AIX, IRIX, or Linux agent from CD-ROM
 - ❖ Installing the HP-UX, AIX, IRIX, or Linux agent from NOW
- ◆ Verifying the installation
 - ❖ Verifying the installation
- ◆ Upgrading from Open Systems SnapVault agent 1.0 to 2.1.1
- ◆ Upgrading from Open Systems SnapVault agent 1.1 or 1.2 to 2.0
- ◆ Upgrading to Open Systems SnapVault agent 2.1.1
- ◆ Uninstalling the Open Systems SnapVault agent
 - ❖ Uninstalling the 1.0 agent
 - ❖ Uninstalling the 1.1, 1.2, 2.0, or 2.1 agent on Windows
 - ❖ Uninstalling the 1.1, 1.2, 2.0 or 2.1 agent on Solaris
 - ❖ Uninstalling the 1.1, 1.2, 2.0 or 2.1 agent on HP-UX, AIX, IRIX, or Linux
- ◆ Configuring and modifying Open Systems SnapVault parameter settings
 - ❖ What the SnapVault Configurator utility does
 - ❖ Running SnapVault Configurator
 - ❖ Confirming that services are running
 - ❖ Enabling and disabling security
 - ❖ Modifying the QSM access list
 - ❖ Modifying the NDMP settings
 - ❖ Reassigning NDMP listen port settings
 - ❖ Generating debugging files
 - ❖ Setting up checksum computation for block-level incremental (BLI) backups
 - ❖ Enabling or disabling BLI backups for certain name-based applications
 - ❖ Configuring OFM
 - ❖ Setting the VSS snapshot timeout parameter on Windows 2003
- ◆ Backing up and restoring Windows System State data
 - ❖ Creating and using System State backups
 - ❖ Primary, authoritative and non-authoritative restores
 - ❖ Disaster Recovery Planning

- ❖ [Adding System State data backup](#)
- ❖ [Restoring System State data from a backup](#)
- ❖ [Restoring System State data from a backup and marking it primary](#)
- ❖ [Preparing disaster recovery backups](#)
- ❖ [Using disaster recovery backups](#)
- ◆ [Open Systems SnapVault relationships](#)
 - ❖ [Deleting and recreating Open Systems SnapVault relationships](#)
 - ❖ [Migrating from one secondary system to another](#)
 - ❖ [Migrating from one volume to another on a secondary system](#)
 - ❖ [Recovering data from a partially initialized transfer](#)
- ◆ [Additional information](#)
 - ❖ [For more information](#)

What you can do with Open Systems SnapVault

The Open Systems SnapVault agent, when installed on your system, enables you to back up data from that system to a Network Appliance™ (NetApp®) secondary storage system using SnapVault technology.

Open Systems SnapVault is used in a manner similar to Data ONTAP™ primary systems to back up and restore data. The most important difference is that with Data ONTAP you can back up or restore only to qtrees using SnapVault. However, with Open Systems SnapVault you can back up and restore to any directory, subdirectory, or volume. Additionally, with Open Systems SnapVault, you can restore a single file. A backed up database can be restored only if no updates occurred between the time the database was backed up and the time it is restored.

See the Data ONTAP *Data Protection Online Backup and Recovery Guide* and the `snapvault` manual (`man`) page for information on using SnapVault technology with Open Systems SnapVault.

Sample backup command: To back up the C: drive of a Windows primary system using Open Systems SnapVault, from the command line of the SnapVault secondary system enter the following command:

```
snapvault start -S winserver:C:\ /vol/volname/winserver_C
```

winserver is the name of the Windows primary system.

/vol/volname/winserver_C is the path on the secondary system to the SnapVault qtree for the backup of the Windows system C: drive.

Sample restore command: To restore a subdirectory from the backup created in the start command above, enter the following command from a Windows shell prompt:

```
"C:\Program Files\netapp\snapvault\bin\snapvault.exe" restore -S  
secondary:/vol/volname/winserver_C/profiles C:\restored
```

C:\Program Files\netapp\snapvault\bin\snapvault.exe is the path to the `snapvault` command on the Windows systems. *secondary* is the name of the secondary system. */vol/volname/winserver_C/* is the path of the qtree on the secondary system that stores the backed up data. *profiles* is the name of the subdirectory in the qtree to be restored. The subdirectory is restored to the Windows system directory *C:\restore*.

What is new with Open Systems SnapVault 2.1.1

Primary fix in Open Systems SnapVault 2.1.1

Open Systems SnapVault 2.1.1 primarily fixes two issues that cause the Open Systems SnapVault backups on Windows to fail with error messages such as the following:

replication destination found a file of improper type

or

replication destination failed to store entry in inode map (on the secondary)

and

failed to generate hybrid history record (on the primary)

The first error message occurs because of improper handling of Windows hard links. The second error occurs because of improper storage of name-based Block Level Increment (BLI) information in the Open Systems SnapVault internal database. For more information, go to <http://now.netapp.com/NOW/cgi-bin/bol/>. Enter bug 151746 in the “Enter Bug ID(s)” text box, and then click Go.

All issues fixed in Open Systems SnapVault 2.1.1

The following table lists the all issues with the Open Systems SnapVault agent (including the one described above) that were fixed in this release. These issues are described in the bug database available at <http://now.netapp.com/NOW/cgi-bin/bol/>. To access information about a specific bug, enter the bug ID in the “Enter Bug ID(s)” text box, and then click Go.

NetApp Bug ID	Description
102790	Alternate data streams that are deleted from a file are not updated to the Secondary
135275	Multiple OSSV Agents may have duplicate NDMP Host IDs
145561	Windows OSSV 2.1 agent unexpectedly transfers large amount of data during an update transfer or the update transfer fails
146086	Hidden attributes of directories get enabled when backed up using OSSV
146654	OSSV NDMP server consumes large amount of memory when port scanner is used

NetApp Bug ID	Description
147054	OSSV backups of UNIX external hard disks may fail with error message "Transfer aborted: source qtree does not exist"
147057	OSSV 2.1 restores fail with error message "Failed to link" when restoring UNIX hard links
149207	OSSV transfers from Windows hang indefinitely
151746	OSSV backups fail with "failed to generate hybrid history record" due to Windows hard links and Name based BLI

Known issue

Open System SnapVault backups on Windows might fail with duplicate inodes due to unknown reasons. For more information, go to <http://now.netapp.com/NOW/cgi-bin/bol/>. Enter bug 156110 in the “Enter Bug ID(s)” text box, and then click Go.

What is new with Open Systems SnapVault 2.1

New features

Open Systems SnapVault 2.1 introduces new features.

The following new Open Systems SnapVault 2.1 features are supported when used with Data ONTAP™ 6.5 software or later:

- ◆ Support for Microsoft Windows 2000 and Windows 2003 System State data backup and restore, including disaster recovery restores.
- ◆ Support for backup exclusion lists.
Open Systems SnapVault agents support both directory and file exclusion lists with wildcards.
- ◆ Support for checkpoint restart on update transfers.
- ◆ Support for backing up Encrypted File System (EFS) encrypted files on Windows 2000 and 2003 systems.

Open Systems SnapVault 2.1 is the first Open Systems SnapVault version that supports backup and restore of EFS encrypted files. Backup of EFS encrypted files requires Data ONTAP 6.5.3P4 or later. See NetApp Bug 139696 for more information.

You can review the text of bug 139696 on the NOW site by entering the bug number 139696 in the Bugs Online Quick Search Enter Bug ID(s) field or enter in your browser the following URL: <http://now.netapp.com/NOW/cgi-bin/bol?Type=Detail&Display=139696>.

For basic Open Systems SnapVault procedures not discussed in these release notes, see the Data ONTAP *Data Protection Online Backup and Recovery Guide* and the snapvault manual (man) page for information on using SnapVault technology with Open Systems SnapVault.

Preinstallation considerations

System requirements for the Open Systems SnapVault agent

Ensure that your site meets the requirements for the primary storage system, the secondary storage system, and the licensing for both systems before you install the Open Systems SnapVault agent.

Primary storage systems:

- ◆ You can install the Open Systems SnapVault 2.1 agent on any of the following 32-bit systems:
 - ❖ Windows Server 2003 Standard Edition and Enterprise Edition on x86 platforms.
 - ❖ Windows 2000 Server and Advanced Server
 - ❖ Windows NT 4 Server Standard Edition, and Enterprise Edition with Service Pack 6
 - ❖ Solaris versions 2.6, 7, 8, and 9
 - ❖ AIX® versions 4.3, 5.1, and 5.2 on POWER systems
 - ❖ Red Hat® Linux versions 7.1, 7.2, 7.3; version 2.1 of the Advanced Server; Red Hat Enterprise Linux AS 3.0, ES 3.0, and WS 3.0
- ◆ You can install the Open Systems SnapVault 2.1 agent on any of the following 64-bit systems:
 - ❖ HP-UX® versions 11 and 11i
The Open Systems SnapVault software running on 64-bit HP-UX systems is 32-bit.
 - ❖ IRIX versions 6.5.x

Note

AMD 64-bit and Itanium systems are not supported.

- ◆ The system must have the following characteristics:
 - ❖ A minimum of 512 MB of memory
 - ❖ For best performance, 100Base-T or Gigabit Ethernet (GbE) TCP/IP connectivity is recommended.
 - ❖ TCP port 10,566 (SnapVault) must be free.

Note

If TCP port 10,000 is already in use, you can reassign it using the SnapVault Configurator user interface. However, you cannot reassign the use of TCP port 10,566.

You need enough disk space for the following:

- ◆ Open Systems SnapVault requires temporary disk space for normal operations. Temporary space of 422 MB is needed for every two million files of 20 KB each during baseline transfer. This number goes up to 601 MB during update transfer if the same number of files are updated.
- ◆ If Open File Manager (OFM) is used, at least 15 percent free disk space in the volume being backed up.
- ◆ Open Systems SnapVault also needs disk space for a built-in database. Database disk space requirements depend on the number and average size of file and number of directories.
 - ❖ If block-level incremental backup is set to OFF:
Size of database = number of files and directories in backup data set x 96 bytes
 - ❖ If block-level incremental backup is set to LOW or HIGH:
Checksums require 16 bytes per 4K bytes of data
Size of database = (number of files and directories in backup data set x 96 bytes) + [total size of all files in the backup data set / (4K bytes x 16 bytes)]
 - ❖ Temporary space = 2 x size of database

Secondary storage systems: To use systems installed with Open Systems SnapVault software, the SnapVault secondary storage system must be running Data ONTAP 6.5.1 or later. However, if you plan to use block-level incremental (BLI) updates, see the discussion about BLI updates in [“Issues and limitations.”](#)

License requirements: You need a SnapVault primary license for each primary storage system whose data you want to back up through SnapVault. The SnapVault primary licenses `sv_windows_pri`, `sv_unix_pri`, or `sv_linux_pri` are installed on the SnapVault secondary storage system.

You need a SnapVault secondary license for the SnapVault secondary storage system.

To back up open files on Windows NT or Windows 2000 using OFM, you need the OFM license for primary storage systems. The OFM license, `sv_windows_ofm_pri`, is installed on your secondary storage system.

To obtain SnapVault or other optional licenses, contact your authorized NetApp® representative.

Issues and limitations

Review the issues and limitations associated with Open Systems SnapVault before you begin using it to back up data.

Issues: The following are known issues with the Open Systems SnapVault agents.

- ◆ Block-level incremental (BLI) backups in Open Systems SnapVault 2.0 might not back up all of the required data when the secondary system is running a version of Data ONTAP that does not have a fix for NetApp Bug 137685. Open Systems SnapVault 2.1 includes a degraded BLI transfer mode that can be used with all versions of Data ONTAP that support Open Systems SnapVault 2.1. Open Systems SnapVault 2.1 automatically determines the BLI mode to use based on the version of Data ONTAP running on the secondary system. See “[Degraded mode BLI transfer](#)” for more information on degraded BLI transfers.

Caution

If you have been using BLI updates on Open Systems SnapVault 2.0, review NetApp Bug 137685 for more information on this problem including a workaround. You can review the text of bug 137685 on the NOW site by entering the bug number 137685 in the Bugs Online Quick Search Enter Bug ID(s) field or entering in your browser the following URL:

<http://now.netapp.com/NOW/cgi-bin/bol?Type=Detail&Display=137685>.

- ◆ The new checkpoint restart for update transfers feature requires an updated version of Data ONTAP running on the secondary system. See NetApp Bug 136194 for information on the required Data ONTAP release levels.
- ◆ When backing up small files, the `snapvault status -l` command might report a backup transfer size significantly greater than the actual size of the file system data being transferred. This happens because of SnapVault protocol overhead (up to 16 KB for each file transferred). This is expected behavior and does not indicate a problem with the backup operation.
- ◆ Open Systems SnapVault supports a maximum of 16 simultaneous transfers on a primary system. You should plan your backup schedules so that 16 or fewer transfers occur at the same time from the same primary system. You can check the number of simultaneous transfers on a system with the command `snapvault status`.

Limitations: Open Systems SnapVault software *does not support* the following:

- ◆ Restore of UNIX sockets

- ◆ Backup and restore of quota database
- ◆ Microsoft 64-bit Windows
- ◆ Installation and configuration of the Open Systems SnapVault agent and data restoration without root access on UNIX® or administrator privileges on a Windows primary storage system
- ◆ Invoking the Open Systems SnapVault software agent outside a secured network
- ◆ FAT and HPFS file systems (only NTFS is supported) on Windows primary storage systems
- ◆ Remote NFS or CIFS file systems that have been mounted on or mapped to UNIX or Windows primary storage systems
- ◆ NFS v4 access control list (ACL) information functionality
- ◆ Multiple file systems in a single operation

Open Systems SnapVault does not cross mount points. You must specify each local mount point as a separate backup if you are backing up multiple file systems. On Windows systems this means mount points that are not mapped to drive letters cannot be backed up.
- ◆ Resync after restore

Open Systems SnapVault does not support the resynchronization of relationships (for example, via `snapvault start -r`) as in NetApp appliance-to-appliance resync. Instead you need to reinitialize the relationship (repeat the original `snapvault start` command) after a restore.

Open Systems SnapVault software does support the following:

- ◆ The following table lists the supported UNIX file systems and those that support ACL backup and restore.

Platform	File systems	Supported ACLs
AIX	JFS*	JFS*
HP-UX	VXFS**, JFS, HFS	HFS
IRIX	XFS	XFS
Linux	EXT2, EXT3	None
Solaris	UFS	UFS

* - Only JFS1 is supported

** - Supported on HP-UX only

Where to find status and problem reports

You can find operational status and problem reports in a log file called *snapvault*. The *snapvault* log file is in the *install_dir* directory. The *install_dir* directory is the one on the primary storage system in which you installed the Open Systems SnapVault agent. The default location for *install_dir* is the c:\Program Files\netapp\snapvault directory. On UNIX systems, the default location for *install_dir* is the /usr directory.

When reporting Open Systems SnapVault agent issues to the NetApp technical support team, send the contents of this log file with your report.

Fixed issues in Open Systems SnapVault 2.1

The following table is a list of issues with the Open Systems SnapVault agent that were fixed in this release and as described in the bug database. For more information, you can go to <http://now.netapp.com/NOW/cgi-bin/bol/>. Enter the Bug ID into the “Enter Bug ID(s)” text box, and then click Go.

NetApp Bug ID	Description
82771	Windows Open Systems SnapVault agent update transfer does not capture ACL changes for files that do not contain modified data

NetApp Bug ID	Description
89010	UNIX Open Systems SnapVault does not update major/minor numbers of special files
106283	Open Systems SnapVault updates fail with incorrect error message
110768	Open Systems SnapVault fails to restore multiple encrypted files in a single directory
111002	Backup of Windows 2003 System Settings with Open Systems SnapVault will stop the Removable Storage Service
130139	Open Systems SnapVault 2.0 fails to release allocated memory on Irix systems
133394	Open Systems SnapVault 2.0 post-script installation failure on Windows systems
134647	Open Systems SnapVault logs a large number of erroneous messages
136264	Large number of concurrent transfers from Open Systems SnapVault resets TCP connection
139557	UNIX and LINUX Open Systems SnapVault agents do not correctly restore files that are multiples of 2MB in size.
140517	Open Systems SnapVault Windows Agents Do Not Back Up and Restore File System Generated Short File Names.
141152	Open Systems SnapVault Database May Significantly Increase In Size With Every Large Update Transfer

Known issues in Open Systems SnapVault 2.1

The following table is a list of known issues with the Open Systems SnapVault agent in this release as described in the bug database. For workarounds or more information, you can go to <http://now.netapp.com/NOW/cgi-bin/bol/>. Enter the Bug ID into the “Enter Bug ID(s)” text box, and then click “Go.”

NetApp Bug ID	Description
83792	Encrypted files backed up using Open Systems SnapVault appear to have zero length
107709	SnapVault status displays incorrect information after filer reboot
115557	snapvault status command on Open Systems SnapVault primary does not display aborted relationship

NetApp Bug ID	Description
117156	Open Systems SnapVault 2.0 must be installed from an ASCII pathname
117223	Using Open Systems SnapVault, if a single file is restored with a trailing slash, a directory is restored

Central management of Open Systems SnapVault agents

You can centrally manage Open Systems SnapVault agents for all operating systems using NetVault™ software with a SnapVault Manager plug-in module from Bakbone® Software, Inc. or using Backup Express software from Syncsort, Inc.

For more information, see the Bakbone Web site at <http://www.bakbone.com/> or the Syncsort Web site at <http://www.syncsort.com/>.

You can also use DataFabric® Manager from all operating systems that support it to centrally manage Open Systems SnapVault agents.

Details of the Open Systems SnapVault 2.1 agent features

Note

For additional information about the `snapvault` command, creating backup schedules, and managing SnapVault and Open Systems SnapVault backups, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

Backup and restore of Windows System State data

Starting with Open Systems SnapVault 2.1, you can now back up and restore the System State data of your Windows 2000 or Windows 2003 system.

Depending on configuration, Windows 2000 and Windows 2003 systems have some or all of the following System State data:

- ◆ Registry
- ◆ COM+ Class Registration database
- ◆ System files, including the boot files
- ◆ Certificate Services database
- ◆ IIS Metadirectory
- ◆ System files that are under Windows File Protection
- ◆ Performance counters

Additionally, the System State data on domain controllers includes Active Directory and SYSVOL data.

See “[Backing up and restoring Windows System State data](#)” for more information.

Backup exclusion lists

New in Open Systems SnapVault 2.1, backup exclusion lists are used by Open Systems SnapVault agents to exclude specified files and directories from backups. Open Systems SnapVault agents support two types of exclusion lists:

- ◆ File exclusion lists
- ◆ Path exclusion lists

File exclusion list entries consist of single path elements. A file or directory is excluded if the file name or any path element matches a file exclusion entry in the list.

Path exclusion list entries consist of complete file system paths to either a directory or a file. If a path exclusion entry specifies a directory, that directory and its files and subdirectories are excluded. A directory path entry must end with a slash (/) on Unix, or a slash (/) or backslash (\) on Windows.

The file exclusion list is in the file *OSSV home/etc/file-exclude.txt*. The path exclusion list is in the file *OSSV home/etc/path-exclude.txt*. On Windows systems, exclusion list files are Unicode text files. On Unix systems, exclusion list files are multibyte text files. Each entry is on its own line. Wildcard characters are supported. Use an asterisk (*) to specify any number of characters within a single path element. Use a question mark (?) to specify one character within a single path element. Use an exclamation mark (!) to remove the special meaning from * or ?. Use a pound sign (#) at the beginning of a line for a comment.

The following is an example of a file exclusion list:

```
# The following excludes any files ending with .tmp.
*.tmp
# The following excludes any directories with a path
# element ending in .tmp.
*.tmp/
# The following excludes Fred, Frad, and so forth, but not
# Freed.
Fr?d
# Exclusion lists on Unix systems are case sensitive,
# but not on Windows systems. So on a Unix system,
# fred would not be excluded, but fred would be excluded on
# Windows systems.
```

The following is an example of a path exclusion list:

```
# The following excludes a file named tmp in the root directory
/tmp
# (On Windows this includes the root directory for all drives.)
# The following excludes a directory named tmp in the root
# directory.
/tmp/
# The following excludes directories in /home, but not files.
/home/*/
# On a Windows system, the following excludes files on the
# C drive, in the My Documents folder, with delete in their
# names. Directories with delete in the path element are not
# excluded. On a Unix system, the entry is invalid and is
# ignored.
C:\My Documents\*delete*
```

The following table includes the complete list of wildcard and special characters.

Character	Meaning
/ or \	Path delimiters for Windows You cannot use ! to escape path delimiters.
/	Path delimiter for Unix You cannot use ! to escape path delimiters.
!	Escape character. Use to escape a following special character. However, you cannot escape a path delimiter.
#	If the first character of a line, the line is a comment.
!n	New line
!r	Carriage return
!t	Tab
!f	Form feed
!b	Backspace
!!	A single !
*	Matches any number of characters, including none. Does not cross path boundaries.
?	Matches any one character.

Checkpoint restart support of update transfers

Open Systems SnapVault 2.0 supported checkpoint restart if the initial baseline backup process failed. Open Systems SnapVault 2.1 adds support for checkpoint restart of update transfers. Checkpoint restart allows a backup transfer to be resumed from a known good point in the backup stream.

Note

Checkpoint restart requires a version of Data ONTAP that has a fix for NetApp Bug 136194. You can review the text of bug 136194 on the NOW site by entering the bug number 136194 in the Bugs Online Quick Search Enter Bug ID(s) field or entering in your browser the following URL:

<http://now.netapp.com/NOW/cgi-bin/bol?Type=Detail&Display=136194>.

Checkpoints are recorded by the primary storage system at periodic intervals or when certain predetermined conditions are met. Checkpoints are taken either at five-minute intervals or at the end of a file. The primary storage system records the checkpoints and sends them to the secondary storage system.

If an update transfer stops because of a retryable error such as a temporary network outage, the transfer is automatically retried. The number of retries is determined by the `tries` option for the relationship. The default tries value is two, which means that a stopped transfer is retried once (the failed initial try counts as the first try). The value can be set with the `-t` option of the `snapvault start` command.

EFS encrypted file backup and restore

Open Systems SnapVault 2.1 supports backing up and recovering EFS encrypted files on Microsoft Windows systems. Backup of EFS encrypted files requires a version of Data ONTAP that has a fix for NetApp Bug 139696. See the following URL to determine the version of Data ONTAP that have a fix for this bug. You can review the text of bug 139696 on the NOW site by entering the bug number 139696 in the Bugs Online Quick Search Enter Bug ID(s) field or entering in your browser the following URL: <http://now.netapp.com/NOW/cgi-bin/bol?Type=Detail&Display=139696>.

If the version of Data ONTAP on your secondary system does not support Open Systems SnapVault backups of EFS encrypted files, Open Systems SnapVault skips those files and creates a log entry listing the skipped files.

Replacing existing EFS files with restored EFS encrypted files requires the Open Systems SnapVault agent to create a temporary file that is equivalent to the size of the EFS encrypted file that is being replaced. Open Systems SnapVault is capable of restoring up to five files concurrently. This means that a restore of EFS encrypted files may require free space in the target Windows volume that is equal to or greater than the sum of the size of the five largest EFS encrypted files in target volume.

EFS encrypted files cannot be backed up using block level incremental backup. Any time an EFS encrypted file is modified, Open Systems SnapVault will back up the entire EFS encrypted file.

Block-level incremental backup

A block-level incremental (BLI) backup recognizes that a file has changed based on a timestamp and checksum algorithm. It also determines exactly which blocks in the file have changed, and then backs up only those blocks to the Open Systems SnapVault secondary storage device during backup transfers. Because

only a small percentage of an application's data changes between periodic backups, incremental backups provide an efficient solution to protecting your data.

Note

BLI does not work on EFS-encrypted files on Windows systems.

Typically, incremental backups are more frequent, reduce the amount of time required to back up data, and minimize the resources required to perform backups when compared to baseline or full backups. This technique significantly reduces the amount of data that needs to be transferred to backup storage, as well as the amount of data that must be stored on backup storage disk.

Caution

Block level increment backups in Open Systems SnapVault 2.0 may not back up all of the required data when the version of Data ONTAP on the filer does not have a fix for NetApp Bug 137685. Open Systems SnapVault 2.1 includes a degraded block level incremental backup mode that can be use with all versions of Data ONTAP that supported Open Systems SnapVault 2.1. Open Systems SnapVault 2.1 automatically determines the block level incremental mode to use based on the version of Data ONTAP running on the secondary. See “[Degraded mode BLI transfer](#)” for more information on degraded BLI transfers. If you have been using BLI updates in Open Systems SnapVault 2.0, review NetApp Bug 137685 for more information on this problem including a workaround. You can review the text of bug 137685 on the NOW site by entering the bug number 137685 in the Bugs Online Quick Search Enter Bug ID(s) field or entering in your browser the following URL: <http://now.netapp.com/NOW/cgi-bin/bol?Type=Detail&Display=137685>.

Recognizing changed blocks: Changed blocks are recognized based on checksum values calculated and preserved for each block by the Open Systems SnapVault primary agent. Checksums are calculated on 4 KB blocks of file data and stored in an internal database.

The checksum database files are stored in the Open Systems SnapVault internal database directory. A separate checksum database file is preserved for each relationship. Disk storage requirements to preserve the calculated checksum values on the primary system are approximately two percent of the baseline backup size.

Individual file timestamps are compared with the time of the last successful backup operation. After a changed file is identified, the checksum calculation is performed for each 4 KB block of the file.

Initial baseline transfer versus incremental updates: You can configure block incremental processing to trade off efficiencies among four variables: primary system CPU utilization, disk consumption, network bandwidth utilization, and Open Systems SnapVault transfer time.

Enabling block-level incremental updates normally causes a checksum value to be calculated for every block of every file during the initial Open Systems SnapVault baseline transfer. As a result, baseline transfer execution time, CPU utilization, disk consumption, and network bandwidth utilization are increased compared to incremental transfers that are not block related. In this case, it is possible that significant resources can be consumed by calculating checksum values for static files that never change. The checksum levels can be configured as high, low, or off, using the `svconfigurator` utility. To configure checksum computation for incremental block-level backups, see “[Setting up checksum computation for block-level incremental \(BLI\) backups](#)”.

To address the static file issue, an option is provided to defer checksum calculations to the incremental update processing. The first time a file changes, the full file is sent to the SnapVault secondary, and checksum values are calculated for each block of that file. The next time the file changes, the checksum comparison is used and only the changed blocks are sent to the secondary. Checksums are calculated only on frequently modified files and during updates.

This heuristic mechanism minimizes execution time, CPU utilization, disk consumption, and network bandwidth utilization during baseline transfers by eliminating checksum calculation and storage for static files. This comes at the expense of some additional SnapVault transfer time for the first incremental update of each changed file.

Degraded mode BLI transfer: Degraded mode BLI transfers are used for BLI transfers to versions of Data ONTAP without the fix for NetApp Bug 137685. If you use BLI in Open Systems SnapVault 2.1, and the secondary system does not have the fix for this problem, Open Systems SnapVault uses degraded BLI transfers automatically. They are not used if the secondary system is running a version of Data ONTAP with the fix. You can review the text of bug 137685 on the NOW site by entering the bug number 137685 in the Bugs Online Quick Search Enter Bug ID(s) field or entering in your browser the following URL: <http://now.netapp.com/NOW/cgi-bin/bol?Type=Detail&Display=137685>.

Degraded mode BLI transfer updates include more blocks of data than standard BLI updates. On Unix systems, the last 4 KB block of a file is always sent, whether the block changed or not. On Windows systems, the last 4 KB block is sent only for the unnamed file stream. All blocks that make up a named file stream are sent as part of the updated transfer.

If you are upgrading from Open Systems SnapVault 2.0 and have been using BLI updates, see NetApp Bug 137685 for more information on the possible loss of data and for repair procedures.

BLI backup of certain name-based files

Open Systems SnapVault 2.1 block-level incremental backup is designed to minimize the backup of data that has not changed since a previous backup operation. Open Systems SnapVault uses checksums to identify portions of a file that have changed between a previous and the current backup.

Appending changes to the end of a file: As part of a block-level incremental backup, Open Systems SnapVault reads each file in the backup data set in 4 KB block increments from beginning to end. During this operation, a checksum is created for each file data block. This checksum is used to track changes between the instance and position of the block in the file that is currently being backed up and the instance and position of the block in this file that was previously backed up.

This technique, shown in the following diagram, works well for backing up changed portions of a file when the application modifies the file by appending changes to the end of the file.

Note

In the following diagrams, the bidirectional arrows indicate file blocks that do not need to be backed up by an Open Systems SnapVault block-level backup.

File being backed up			File previously backed up	
Start Offset 0	Checksum 0	↔	Start Offset 0	Checksum 0
Start Offset 4k	Checksum 1	↔	Start Offset 4k	Checksum 1
Start Offset 8k	Checksum 2	↔	Start Offset 8k	Checksum 2
Start Offset 12k	Checksum 5		Start Offset 12k	Checksum 3
Start Offset 16k	Checksum 4	↔	Start Offset 16k	Checksum 4

File being backed up			File previously backed up	
Start Offset 0	Checksum 0	↔	Start Offset 0	Checksum 0
Start Offset 4k	Checksum 1	↔	Start Offset 4k	Checksum 1
Start Offset 8k	Checksum 2	↔	Start Offset 8k	Checksum 2
Start Offset 12k	Checksum 3	↔	Start Offset 12k	Checksum 3
Start Offset 16k	Checksum 4	↔	Start Offset 16k	Checksum 4
Start Offset 20k	Checksum 5			

In some cases, applications modify files by

1. Creating a temporary copy of the original file
2. Making the necessary changes to that temporary file
3. Deleting the original file
4. Saving the temporary file under the same name as the original file

Open Systems SnapVault can detect this condition and treat the new instance of the renamed temporary file as the updated original file.

Rewriting subsequent data blocks: In certain cases, applications make changes, as shown in the following diagram, to files by

1. Inserting data into or removing data from the middle of the file
2. Rewriting all subsequent data blocks in the file to new positions in the file

File being backed up		↔	File previously backed up	
Start Offset 0	Checksum 0		Start Offset 0	Checksum 0
Start Offset 4k	Checksum 5		Start Offset 4k	Checksum 1
Start Offset 8k	Checksum 6		Start Offset 8k	Checksum 2
Start Offset 12k	Checksum 7		Start Offset 12k	Checksum 3
Start Offset 16k	Checksum 8		Start Offset 16k	Checksum 4
Start Offset 20k	Checksum 9			

Microsoft Word, Excel, and PowerPoint are some of the applications that are known to exhibit this behavior when saving changes to files. For files that are modified in this manner, Open Systems SnapVault backs up all blocks in the file that have different positions or different checksum values.

Open Systems SnapVault agents have a different capability to work around this issue. Unlike the corresponding filer option, it is enabled by default. To enable or disable the workaround, see [“Enabling or disabling BLI backups for certain name-based applications”](#).

Windows NT and Windows 2000 OFM option

The Open File Manager (OFM) utility allows Windows NT and Windows 2000 files that are open and in use to be backed up with only a very short disruption to users or their current applications. OFM is automatically installed in your system at the same time the agent is installed. To configure OFM, see [“Configuring OFM”](#) on page 54.

Windows 2003 VSS snapshots

Windows Server 2003 provides a native snapshot mechanism as part of the Volume Shadow Copy Service (VSS). VSS snapshot functionality (called shadow copy) is integrated with the Open Systems SnapVault agent as a standard feature. Windows Server 2003 Open Systems SnapVault agent backups use VSS.

You can set the amount of time (snapshot timeout) that the agent waits until it retries a VSS snapshot if the conditions are not right at the time. To set the VSS snapshot timeout parameter, see [“Setting the VSS snapshot timeout parameter on Windows 2003”](#).

SnapVault secondary protection using SnapMirror

You can now protect against disasters on the SnapVault secondary system by using the SnapMirror® feature. The configuration involves setting up SnapMirror relationships from the volumes on your SnapVault secondary system to volumes on a remote (tertiary) Data ONTAP system. SnapMirror thus provides an exact replica of the SnapVault secondary data on the tertiary system.

Additionally, softlock support in Open Systems SnapVault 2.1 enables you to continue SnapVault replication relationships between the original SnapVault primary system and the tertiary system, without any initial baseline transfers. For instance, if your SnapVault secondary system becomes unusable because of a disaster, you can manually redirect your next SnapVault transfers to the tertiary system instead of the old SnapVault secondary system. Effectively, your tertiary system becomes the new SnapVault secondary system, and your SnapVault transfers continue using the latest “snapshot” common to both the primary and the tertiary systems.

“Snapshot” is in quotes in the preceding sentence because Open Systems SnapVault primary systems do not literally keep Snapshot™ copies. They keep the equivalent state in a database that allows the Open Systems SnapVault primary system to perform many operations equivalent to those of a filer primary system. This document hereafter refers to the “state” as a snapshot. For more information about using SnapMirror, see the Data ONTAP *Data Protection Online Backup and Recovery Guide*.

Checkpoint restart of initial transfers

When an Open Systems SnapVault initial baseline backup process fails, checkpoint restart support allows the baseline backup transfer to be resumed from a known good point in the backup stream.

Checkpoints are recorded by the primary storage system when certain predetermined conditions or periodic intervals are met. Checkpoints are taken either at five-minute intervals or at the end of a file, whichever happens later. The primary storage system records the checkpoints and sends them to the secondary storage system.

The snapvault command on the primary storage system

The snapvault command replaces the Open Systems SnapVault 1.x svrestore command and adds extra capabilities, including abort, destinations, help, release, restore, and status.

You can run the help system on the primary storage system using the command-line interface. To run help, you enter the `snapvault help` command. For example, to get help on the `status` command syntax, you enter

`snapvault help status`

Installing Open Systems SnapVault agents on Windows platforms

Installing a Windows agent from CD-ROM

To install the Open Systems SnapVault Windows NT, Windows 2000, or Windows 2003 agent on your supported Windows primary storage system from CD-ROM, complete the following steps.

Note

For Windows NT and Windows 2000, St. Bernard's OFM module requires that you reboot the system after installation. If you choose not to reboot the system after installation, you will be unable to use OFM's Open File Backup functionality until you reboot the system.

Step	Action
1	Log in to your Windows primary storage system with Administrator privileges.
2	Insert the CD-ROM labeled <i>Open Systems SnapVault Agent</i> into the primary storage system's CD-ROM drive.
3	From the command line or Windows Explorer, navigate to the CD-ROM directory specific to your platform: ◆ For Windows NT, go to \NT. ◆ For Windows 2000, go to \WIN2K. ◆ For Windows 2003, go to \WIN2K3 Depending on your system configuration, the files and directories mentioned might appear in lowercase characters. To navigate to the correct directory, use uppercase characters for the directory name (for example, cd \WIN2K).
4	After navigating to the appropriate directory for your platform, see "Using the Installation Wizard" to complete the installation.

Installing a Windows agent from NOW

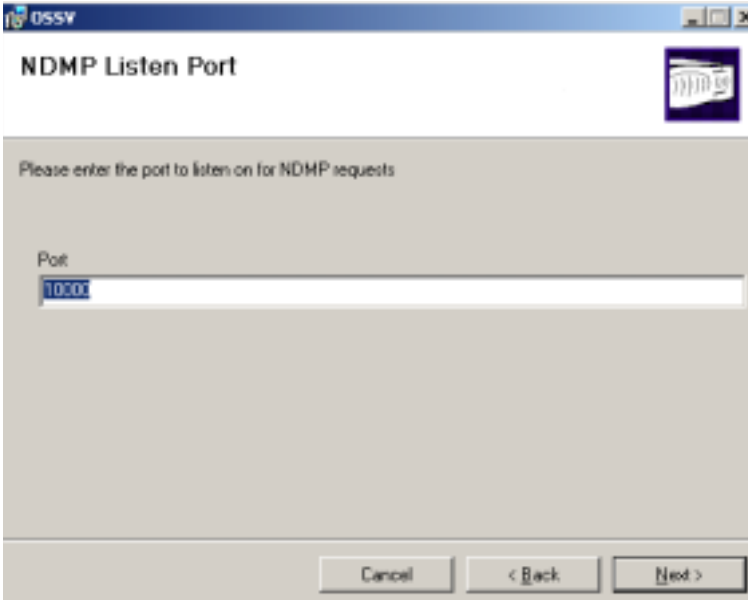
To download the Open Systems SnapVault Windows agent module from the NetApp on the Web™ (NOW™) site and install the agent on your supported Windows platform, complete the following steps.

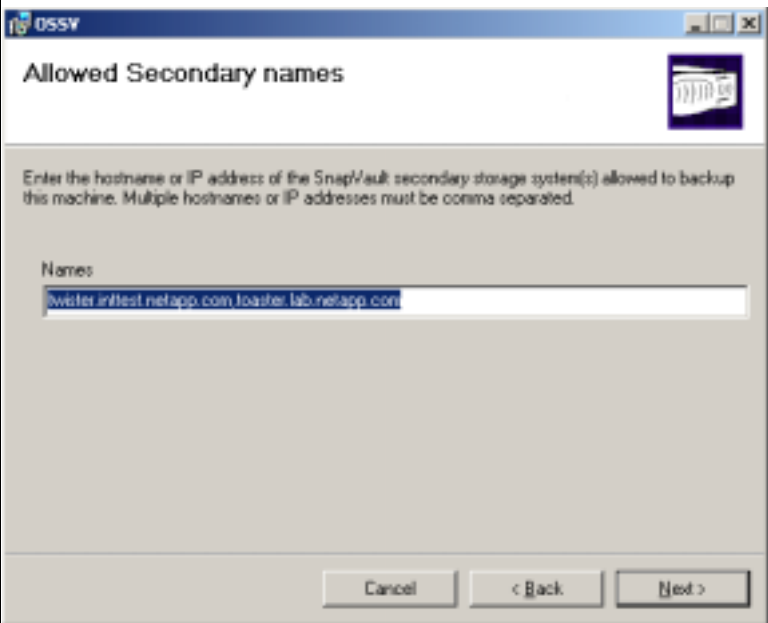
Step	Action
1	Log in to your primary storage system with Administrator privileges.
2	Go to the Download Software page of the NOW site at http://now.netapp.com/Self-Service/Personal/usrPage.asp , and follow the directions to download the appropriate Open Systems SnapVault package.
3	Transfer one of the following zip packages for your Windows operating system to your local system: ossv_nt_v2.1.zip, ossv_win2k_v2.1.zip, or ossv_win2k3_v2.1.zip.
4	After you transfer the appropriate Open Systems SnapVault package, extract the files into any temporary directory. ◆ On Windows NT primary storage systems—Unzip the downloaded ossv_nt_v2.1.zip package. ◆ On Windows 2000 primary storage systems—Unzip the downloaded ossv_win2k_v2.1.zip package. ◆ On Windows 2003 primary storage systems—Unzip the downloaded ossv_win2k3_v2.1.zip package.
5	After navigating to the appropriate directory for your platform, see “ Using the Installation Wizard ” to complete the installation.

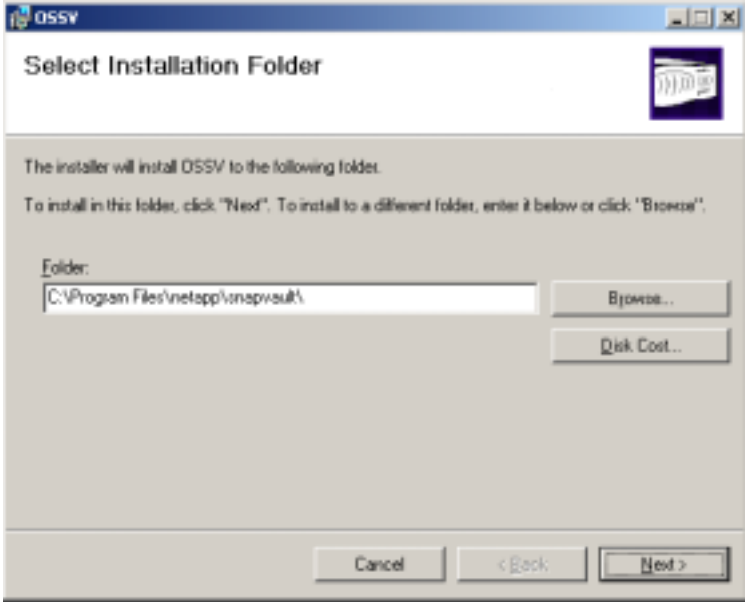
Using the Installation Wizard

To use the Installation Wizard to install the Open Systems SnapVault agent on your system, complete the following steps.

Step	Action
1	Locate and double-click the setup.exe file. Result: The Open Systems SnapVault Setup Wizard is launched.
2	Follow the instructions on the screen. Click the “I Agree” radio button to accept the license agreement and click Next. Result: The Choose NDMP Username/Password window appears.

Step	Action
3	Optional: Enter your user name and password, retype your password to confirm it, and click Next. Result: The NDMP Listen Port window appears. Or, simply click Next.
4	Enter the NDMP listening port in the NDMP Listen Port window when prompted, or accept the default listening port setting of 10,000, and click Next.  If another application uses 10,000 as its listening port, choose a port number greater than 10,000 that is currently not being used.

Step	Action
5	When the “Allowed Secondary Names” window appears and you are prompted for allowed secondary storage system names, enter one or more host names or IP addresses of the SnapVault secondary storage system or systems that you want to back up this primary storage system.  Note If you specify multiple SnapVault secondary storage systems, separate the host names or IP addresses with commas. Only the secondary storage systems named in this field are accepted by the primary system as valid backup systems.

Step	Action
6	When the Select Installation Folder window prompts you for the installation directory, click Next to accept the default location, or enter your own path to a different folder and click Next.  If the Open Systems SnapVault agent was previously installed and then uninstalled, files might still be resident in the installation directory and a dialog box appears. To empty the directory, click Yes in the dialog box before you click Next. Click Disk Cost to view the available disk space. Result: The Confirm Installation window appears to inform you that the installer is ready to install Open Systems SnapVault on your computer.
7	Click Next to start the installation process and wait until the Installation Complete window appears, then click Close.

Step	Action	
8	For Windows NT or 2000...	For Windows 2003...
	Reboot the system when prompted if you plan to use OFM; otherwise, go to Step 9.	Go to step 9.
9	After you finish installing the Open Systems SnapVault agent, follow the procedures in the SnapVault chapter of the Data ONTAP <i>Data Protection Guide</i> to configure the SnapVault secondary storage system for Open Systems backup.	

Remote batch installation of the Open Systems SnapVault agent on Windows

Remote installation of the Open Systems SnapVault agent onto Windows clients is based on the Windows domain and active directory. Remote installation of the Open Systems SnapVault agent is supported.

In active directory, an administrator establishes a policy to push the Open Systems SnapVault agent onto a number of clients within the domain. When those clients are rebooted, the agent is installed.

For information about remote batch installation in the Windows environment, see <http://www.microsoft.com/>.

Installing Open Systems SnapVault agents on Solaris, HP-UX, AIX, IRIX, or Linux platforms

Installing the Solaris agent from CD-ROM

To install the Open Systems SnapVault Solaris agent on your supported UNIX primary storage system from CD-ROM, complete the following steps.

Step	Action
1	Log in to your primary storage system as root.
2	Insert the CD-ROM labeled <i>Open Systems SnapVault Agent</i> into the primary storage system's CD-ROM drive.
3	Navigate to the Solaris pkgadd package on the CD-ROM.
4	Run the Solaris pkgadd utility using the following command: pkgadd -d ossv Result: The package installation script is initiated and asks you a series of questions prior to and during the installation process.
5	Go to “ Using the Solaris pkgadd utility to install the Solaris agent ” to continue the Solaris package installation.

Installing the Solaris agent from NOW

To download this software module from the NOW site and install the Open Systems SnapVault Solaris agent, complete the following steps.

Step	Action
1	Log in to your primary storage system as root.
2	Go to the Download Software page of the NOW site at http://now.netapp.com/Self-Service/Personal/usrPage.asp , and follow the directions to download the Open Systems SnapVault Solaris agent package.

Step	Action
3	After you download the Open Systems SnapVault package, unpack and start the installation program as follows: ◆ On Solaris primary storage systems—Uncompress and untar the downloaded pkgadd package. ◆ Run the Solaris pkgadd utility using the following command: pkgadd -d ossv Result: The package installation script starts and asks you a series of questions prior to and during the installation process.
4	Go to “Using the Solaris pkgadd utility to install the Solaris agent” to continue the Solaris package installation.

Using the Solaris pkgadd utility to install the Solaris agent

The Solaris pkgadd utility transfers the contents of a software package from the distribution medium or directory to install it onto the system.

To install the Open Systems SnapVault Solaris agent using the pkgadd package, complete the following steps.

Step	Action
1	Answer yes (y), no (n), or display (d) when asked if you read and agreed to the terms of the license. If you answer no (n), you cannot install the package.
2	When prompted, enter the path where you want the SnapVault directory to be created. The default directory is /usr/snapvault. If the directory you entered already exists, you are warned that the current contents of that directory will be destroyed if you continue and then prompted whether you want to continue. Enter yes (y) or no (n).
3	Enter your user name to connect to the target system using the NDMP protocol.
4	Enter and confirm the password to connect to the system.
5	Enter the NDMP listener port. The default listener port is 10,000.

Step	Action
6	Enter the host names or IP addresses of the SnapVault secondary storage systems that are allowed to perform backups to this primary storage unit.
7	A series of installation scripts is executed. If successful, the following message appears: Installation of OSSV was successful.

Installing the HP-UX, AIX, IRIX, or Linux agent from CD-ROM

To install the Open Systems SnapVault HP-UX, AIX, IRIX, or Linux agent on your supported UNIX primary storage system from CD-ROM, complete the following steps.

Step	Action
1	Log in to your primary storage system as root.
2	Insert the CD-ROM labeled <i>Open Systems SnapVault Agent</i> into the primary storage system's CD-ROM drive.
3	From the command line, navigate to the CD-ROM directory specific to your platform: ◆ For HP-UX, go to /HPUX. ◆ For AIX, go to /AIX. ◆ For IRIX, go to /IRIX ◆ For Linux, go to /LINUX. Depending on your system configuration and mount options, the files and directories mentioned might appear in lowercase characters.
4	From the command line, enter the following command using all uppercase characters: INSTAL
5	When the INSTAL program prompts for the Installation directory, press Enter to accept the default, or enter your own path. The default value, /usr, installs the Open Systems SnapVault software in /usr/snapvault.

Step	Action	
6	If you plan to manage SnapVault backup through...	Then...
	Your Data ONTAP command line	Press Enter.
	A commercial NDMP application	When the INSTAL program prompts you for the user name, password, and NDMP listening port, specify a user name and password authorized through that application.
7	When the INSTAL program prompts you for Allowed Systems, enter one or more host names or IP addresses of the SnapVault secondary storage system or systems that you want to back up this primary storage system. Note If you specify multiple SnapVault secondary storage systems, separate the host names or IP addresses with commas.	
8	Look for a message similar to the following that is displayed to indicates a successful installation: Installation completed successfully. The message also refers to a log file. The log file is created when the first SnapVault backup occurs, not by the installation process. Therefore, if you search for the log file after completing the installation but before you back up data for the first time, you will not find the log file. Note Installation messages are sent directly to the console and are not captured in any log file. Error messages that occurred during the installation process are logged in the log file.	

Step	Action
9	After you finish installing the Open Systems SnapVault agent, follow the procedures in the SnapVault chapter of the Data ONTAP <i>Data Protection Guide</i> to configure the SnapVault secondary storage system for Open Systems SnapVault backup.

Installing the HP-UX, AIX, IRIX, or Linux agent from NOW

To download the Open Systems SnapVault HP-UX, AIX, IRIX, or Linux agent from the NOW site and install it, complete the following steps.

Step	Action
1	Log in to your primary storage system as root.
2	Go to the Download Software page of the NOW site at http://now.netapp.com/Self-Service/Personal/usrPage.asp , and follow the directions to download the appropriate Open Systems SnapVault package.

Step	Action
3	After you download the Open Systems SnapVault package, unpack and start the installation program as follows: ◆ On HP-UX primary storage systems—Uncompress and untar the downloaded <code>ossv_hpux_v2.1.tar.Z</code> package using the following commands: <pre>uncompress ossv_hpux_v2.1.tar.Z tar -xvf ossv_hpux_v2.1.tar</pre> ◆ On AIX primary storage systems—Uncompress and untar the downloaded <code>ossv_aix_v2.1.tar.Z</code> package using the following commands: <pre>uncompress ossv_aix_v2.1.tar.Z tar -xvf ossv_aix_v2.1.tar</pre> ◆ On IRIX primary storage systems—Uncompress and untar the downloaded <code>ossv_irix_v2.1.tar.Z</code> package using the following commands: <pre>uncompress ossv_irix_v2.1.tar.Z tar -xvf ossv_irix_v2.1.tar</pre> ◆ On Linux primary storage systems—Uncompress and untar the downloaded <code>ossv_linux_v2.1.tar.Z</code> package using the following commands: <pre>uncompress ossv_linux_v2.1.tar.Z tar -xvf ossv_linux_v2.1.tar</pre>
4	Enter the following command sequence: <pre># cd SnapVaultDistribution # ./SVINSTAL</pre>
5	When the INSTAL program prompts for the Installation directory, press Enter to accept the default, or enter your own path. The default value, <code>/usr</code>, installs the Open Systems SnapVault software in <code>/usr/snapvault</code>.

Step	Action	
6	If you plan to manage SnapVault backup through...	Then...
	Your Data ONTAP command line	Press Enter.
	A commercial NDMP application	When the INSTAL program prompts you for the user name, password, and NDMP listening port, specify a user name and password authorized through that application.
7	When the INSTAL program prompts you for Allowed Systems, enter one or more host names or IP addresses of the SnapVault secondary storage system or systems that you want to back up this primary storage system. Note_____ If you specify multiple SnapVault secondary storage systems, separate the host names or IP addresses with commas but no spaces. _____	
8	After you finish installing the Open Systems SnapVault agent, follow the procedures in the SnapVault chapter of the Data ONTAP <i>Data Protection Guide</i> to configure the SnapVault secondary storage system for Open Systems backup.	

Verifying the installation

Verifying the installation

To ensure that the installation was completed correctly and that the primary and secondary storage systems can back up data, complete the following steps.

Step	Action
1	Verify connectivity to the secondary storage system using the following command: ping <i>secondary_system</i> <i>secondary_system</i> is either the name or the IP address of the secondary storage system.
2	If security was enabled during installation, ensure that the secondary storage system specified is accessible from the primary storage systems, using the procedure described in “ Enabling and disabling security ”.
3	Ensure that the volumes you need were created on the secondary storage system before you attempt to back up data to them. Note — The volumes should not have qtrees already created.
4	If there are firewalls between the primary storage system and the secondary storage system, ensure that TCP port 10,000 and 10,566 are allowed using the <code>telnet</code> command. TCP port 10,566 is used by the SnapVault process and TCP port 10,000 is used by NDMP applications.
5	Navigate to <i>install_dir</i> /bin/svinstallcheck and run <code>svinstallcheck</code> to verify successful installation and to make sure that the services are running properly. <i>install_dir</i> is the location where you installed the Open Systems SnapVault agent.

Upgrading from Open Systems SnapVault agent 1.0 to 2.1.1

Upgrading the 1.0 agent

To upgrade the Open Systems SnapVault 1.0 agent to 2.1.1, complete the following steps.

Step	Action
1	To ensure that your Open Systems SnapVault database is not accidentally removed during installation, move the database directory to a new location or back it up using the procedure in the <i>Data ONTAP Data Protection Online Backup and Recovery Guide</i> .
2	Uninstall Open Systems SnapVault 1.0 using the procedure described in “Uninstalling the 1.0 agent” .
3	Install the Open Systems SnapVault 2.1.1 agent using the procedure described in “Installing Open Systems SnapVault agents on Windows platforms” or “Installing Open Systems SnapVault agents on Solaris, HP-UX, AIX, IRIX, or Linux platforms”. Result: The agent automatically starts Open Systems SnapVault services after installation.
4	Stop Open Systems SnapVault services by invoking the SnapVault svconfigurator utility, clicking the Service tab, and then clicking Stop Service. Note The svpmgr shutdown command can be used as an alternative only on UNIX systems.
5	Copy the database directory that you saved in Step 1 to the location of the database created by the new installation.

Step	Action
6	Start Open Systems SnapVault services by invoking the SnapVault svconfigurator utility, clicking the Service tab, and then clicking Start Service. Note_____ The svpmgr command can be used as an alternative only on UNIX systems. _____

Upgrading from Open Systems SnapVault agent 1.1 or 1.2 to 2.0

Upgrading the 1.1 or 1.2 agent

Note

You cannot upgrade from a beta version to a release version. If you have a beta version installed, remove it following the appropriate procedure in the section [“Uninstalling the Open Systems SnapVault agent.”](#)

To upgrade the Open Systems SnapVault 1.1 or 1.2 to 2.0 agent, complete the following steps.

Note

If an Open Systems SnapVault 1.2 agent is upgraded to 2.0, then the Enable Unix ACLs tab appears in the svconfigurator. Ignore this tab because it has no effect on agent functionality. When upgrading to an Open Systems SnapVault 2.0 agent from either an Open Systems SnapVault 1.0 or 1.1 agent, this tab does not appear in the svconfigurator.

Step	Action
1	Stop Open Systems SnapVault services by invoking the SnapVault Configurator utility, clicking the Service tab, and then clicking Stop Service.
2	To ensure that your Open Systems SnapVault database is not accidentally removed during installation, move the database directory to a new location or back it up using the procedure in the <i>Data ONTAP Data Protection Online Backup and Recovery Guide</i> .
3	Install the Open Systems SnapVault 2.0 agent using the procedure described in “Installing Open Systems SnapVault agents on Windows platforms” or “Installing Open Systems SnapVault agents on Solaris, HP-UX, AIX, IRIX, or Linux platforms” . Result: The agent automatically starts Open Systems SnapVault services after installation.
4	Stop Open Systems SnapVault services, as described in Step 1.
5	Restart Open Systems SnapVault services by invoking the SnapVault Configurator utility, clicking the Service tab, clicking Start Service, and then clicking OK.

Upgrading to Open Systems SnapVault agent 2.1.1

Upgrading the 1.1 or 1.2 agent

Note

You cannot upgrade from a beta version to a release version. If you have a beta version installed, remove it following the appropriate procedure in the section [“Uninstalling the Open Systems SnapVault agent.”](#)

Upgrading an Open Systems SnapVault 1.1 or 1.2 agent to 2.1.1 is a two step process. First you must upgrade to 2.0, then you upgrade to 2.1.1. Upgrading to 2.0 is described in [“Upgrading from Open Systems SnapVault agent 1.1 or 1.2 to 2.0”](#) on page 42.

Upgrading the 2.0 or 2.1 agent

To upgrade the Open Systems SnapVault 2.0 or 2.1 agent to the Open Systems SnapVault 2.1.1 agent, complete the following steps.

Note

If you are upgrading from Open Systems SnapVault 2.0 and have been using BLI updates, or do not know if you have been using BLI updates, review NetApp Bug 137685 for information about a problem in some versions of Data ONTAP that can cause lose of data in Open Systems SnapVault 2.0 BLI updates and see [“Degraded mode BLI transfer”](#) for information on a workaround for this problem included with Open Systems SnapVault 2.1.

Step	Action
1	Stop Open Systems SnapVault services by invoking the SnapVault Configurator utility, clicking the Service tab, and then clicking Stop Service.
2	To ensure that your Open Systems SnapVault database is not accidentally removed during installation, move the database directory to a new location or back it up using the procedure in the <i>Data ONTAP Data Protection Online Backup and Recovery Guide</i> .

Step	Action
3	Install the Open Systems SnapVault agent using the procedure described in “Installing Open Systems SnapVault agents on Windows platforms” or “Installing Open Systems SnapVault agents on Solaris, HP-UX, AIX, IRIX, or Linux platforms”. Result: The agent automatically starts Open Systems SnapVault services after installation.
4	Stop Open Systems SnapVault services, as described in Step 1.
5	Restart Open Systems SnapVault services by invoking the SnapVault Configurator utility, clicking the Service tab, clicking Start Service, and then clicking OK.

Uninstalling the Open Systems SnapVault agent

Uninstalling the 1.0 agent

To uninstall the Open Systems SnapVault 1.0 agent, complete the following steps.

Step	Action
1	Using the command line interface of the Open Systems SnapVault primary system, navigate to the <i>snapvault/util</i> directory. ◆ On Windows systems, the default path is: C:\Program Files\snapvault\util ◆ On UNIX systems, the default path is: /usr/snapvault/util
2	Enter the following command: svuninstall
3	After the command is complete, remove the <i>snapvault</i> directory.

Uninstalling the 1.1, 1.2, 2.0, or 2.1 agent on Windows

To uninstall the Open Systems SnapVault 1.1, 1.2, 2.0, or 2.1 agent on the Windows platform, complete the following steps.

Step	Action
1	Click Start > Control Panel.
2	Double-click Add or Remove Programs.
3	Choose the Open Systems SnapVault agent in the list of programs and click Remove. Result: Windows uninstalls the Open Systems SnapVault agent and responds with a message to inform you that the uninstall is successful.

Uninstalling the 1.1, 1.2, 2.0 or 2.1 agent on Solaris

To uninstall the Open Systems SnapVault 1.1, 1.2, 2.0 or 2.1 agent on a Solaris platform, complete the following steps.

Step	Action
1	Log in to your primary storage system as root.
2	Run the pkgrm utility: pkgrm ossv
3	Answer yes (y) when asked whether you want to remove this package. The script responds with the following text: ## Removing installed package instance <ossv> This package contains scripts which will be executed with super-user permission during the process of removing this package.
4	Answer yes (y) when asked whether you want to continue with the removal of this package. Result: If removal is successful, the script responds with the following text: Removal of <ossv> was successful.

Uninstalling the 1.1, 1.2, 2.0 or 2.1 agent on HP-UX, AIX, IRIX, or Linux

To uninstall the Open Systems SnapVault 1.1, 1.2, 2.0 or 2.1 agent on the HP-UX, AIX, IRIX, or Linux platform, complete the following steps.

Step	Action
1	Using the command-line interface of the Open Systems SnapVault primary storage system, navigate to the location of the agent (the default location is usr/snapvault/util).
2	Enter the following command: uninstall
3	If the snapvault directory still appears after running uninstall, remove the directory manually.

Configuring and modifying Open Systems SnapVault parameter settings

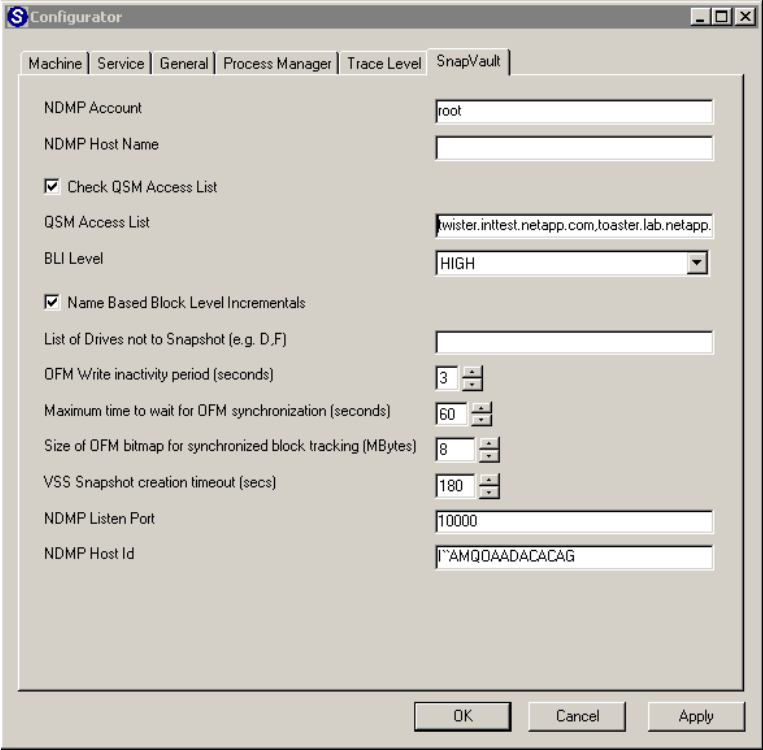
What the SnapVault Configurator utility does

If you need to modify any of the default parameter settings, you can invoke the SnapVault Configurator (svconfigurator) utility through the command-line interface or launch the graphical user interface (GUI) on the system on which you installed the Open Systems SnapVault agent. You can perform the following procedures from the SnapVault Configurator utility:

- ◆ [Confirming that services are running](#)
- ◆ [Enabling and disabling security](#)
- ◆ [Modifying the QSM access list](#)
- ◆ [Modifying the NDMP settings](#)
- ◆ [Reassigning NDMP listen port settings](#)
- ◆ [Generating debugging files](#)
- ◆ [Setting up checksum computation for block-level incremental \(BLI\) backups](#)
- ◆ [Enabling or disabling BLI backups for certain name-based applications](#)
- ◆ [Configuring OFM](#)

Running SnapVault
Configurator

To run SnapVault Configurator, complete the following steps.

Step	Action
1	To launch the SnapVault GUI, you can either ◆ Use the command-line interface of the Open Systems SnapVault primary storage system, navigate to <i>install_dir</i>\bin, and invoke <i>svconfigurator</i>, or ◆ Use Windows Explorer to navigate to Start > Programs > OSSV > OSSV Configurator The most commonly modified parameters are accessed by clicking the SnapVault tab shown in the following window. 
2	Click the appropriate SnapVault Configurator tab to change the settings.
3	Click the Service tab, click Stop Service, click Start Service, and then click OK.

Confirming that services are running

To confirm that Open Systems SnapVault services are running, complete the following steps.

Step	Action
1	Click the Service tab.
2	Verify that Current State Running is shown.
3	If services are not running, click Start Service.
4	Click OK.

Enabling and disabling security

As a security measure, Open Systems SnapVault uses an access list to determine the secondary storage systems to which the primary storage system has permission to back up data. To enable or disable security, complete the following steps.

Step	Action
1	Click the SnapVault tab.
2	Click the Check QSM Access List box to enable or disable security.
3	Click OK.

Modifying the QSM access list

You can change the secondary storage systems to which the primary storage system backs up data by modifying the Qtree SnapMirror (QSM) access list. To modify the QSM access list, complete the following steps.

Step	Action
1	Click the SnapVault tab.
2	You can add to, replace, or delete IP addresses or host names of the secondary storage systems to which you want to back up data.
3	Click OK.

Modifying the NDMP settings

The NDMP host name is used by both the primary and secondary storage systems to identify the Open Systems SnapVault agent and its associated snapshots. The NDMP host name field is automatically filled in with a unique name created by the Open Systems SnapVault installation program and must not be modified. To modify the NDMP account name, complete the following steps.

Step	Action
1	Click the SnapVault tab.
2	Modify the NDMP account name in the window.
3	Click OK. Note _____To change the password, use the command line. Navigate to the <i>install_dir\bin</i> directory and run the <i>svpassword</i> command to change the password. _____

Reassigning NDMP listen port settings

To reassign the NDMP listen port default setting of 10,000 to another unused port number, complete the following steps.

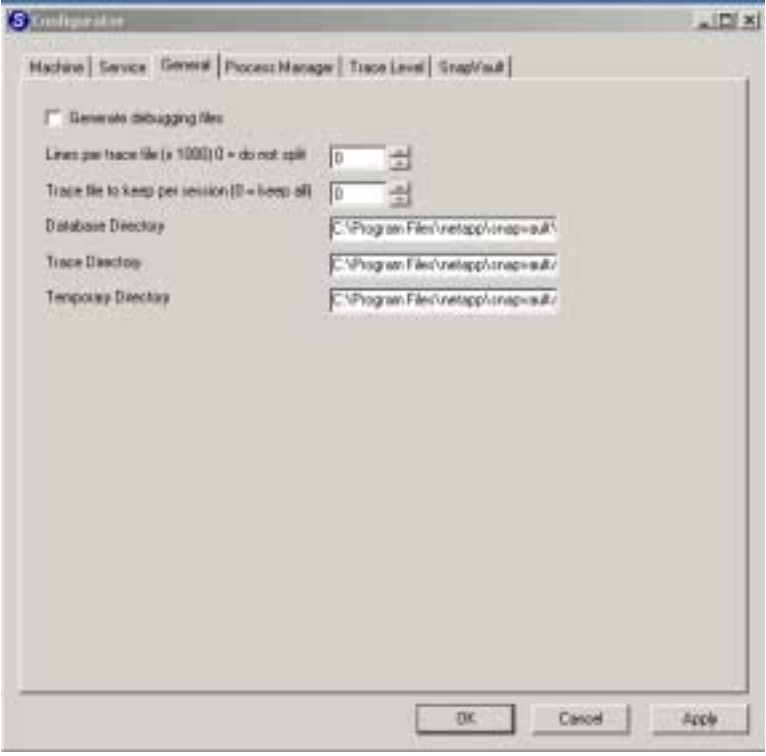
Step	Action
1	Click the SnapVault tab.
2	In the NDMP Listen Port box, enter an unused TCP port number.
3	Click OK.
4	Stop and restart services after assigning the NDMP listen port.

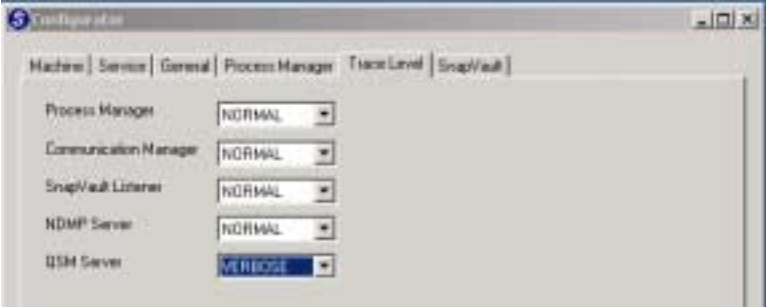
Generating debugging files

You can generate debugging files to help troubleshoot problems, but you should generate these files only with the assistance of NetApp Technical Support.

Caution_____Debugging files grow large quickly and there is a performance impact; therefore, you should only generate debugging files when you need them.

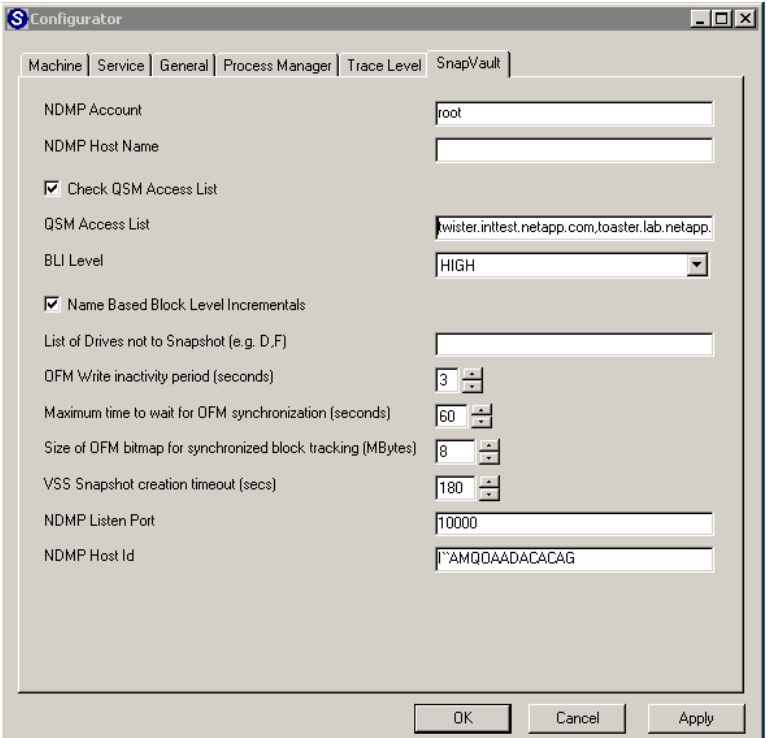
To generate debugging files, complete the following steps.

Step	Action
1	Click the General tab, shown in the following window.
	
2	Select the “Generate debugging files” check box.
3	Click the Trace Level tab.

Step	Action
4	For QSM Server, select VERBOSE, as shown in the following window.  The screenshot shows a window titled 'Configuration' with several tabs: Machine, Service, General, Process Manager, Trace Level, and SnapVault. The 'Process Manager' tab is selected. It contains five dropdown menus: Process Manager (NORMAL), Communication Manager (NORMAL), SnapVault Listener (NORMAL), NDMP Server (NORMAL), and QSM Server (VERBOSE). The QSM Server dropdown is highlighted with a blue selection bar.
5	Click Apply.
6	Click the Service tab, click Stop Service, click Start Service, and then click OK.

Setting up
checksum
computation for
block-level
incremental (BLI)
backups

You can choose the level at which you want to compute BLI checksums or you can disable checksum computations entirely. To choose the level of BLI checksum computation or to disable it, complete the following steps.

Step	Action
1	Click the SnapVault tab, as shown in the following window. The block-level incremental checksum computation options are displayed in the BLI Level drop-down menu. 

Step	Action
2	Choose the block-level (BLI Level) option you want using the drop-down menu. ◆ HIGH—computes checksums during the initial baseline backup and updates Note _____ The HIGH mode might slow down the initial backup transfer. ◆ LOW—computes checksums only during updates ◆ OFF—disables block-level incremental backups altogether

Enabling or disabling BLI backups for certain name-based applications

Block-level incremental backups for certain name-based applications, such as Microsoft's productivity applications, are enabled by default. To enable or disable this block-level incremental backup feature, complete the following steps.

Step	Action
1	Click the SnapVault tab.
2	To enable or disable block-level incremental backup, select or clear the Select Block Level Incrementals option.

Configuring OFM

OFM waits for a set time when write activity is quiet and the system is in a safe state to initiate the backup of open files. OFM listens continuously for a period of write inactivity until it is ready to initiate a synchronize for backup or until the preset synchronization timeout period has expired.

Note _____

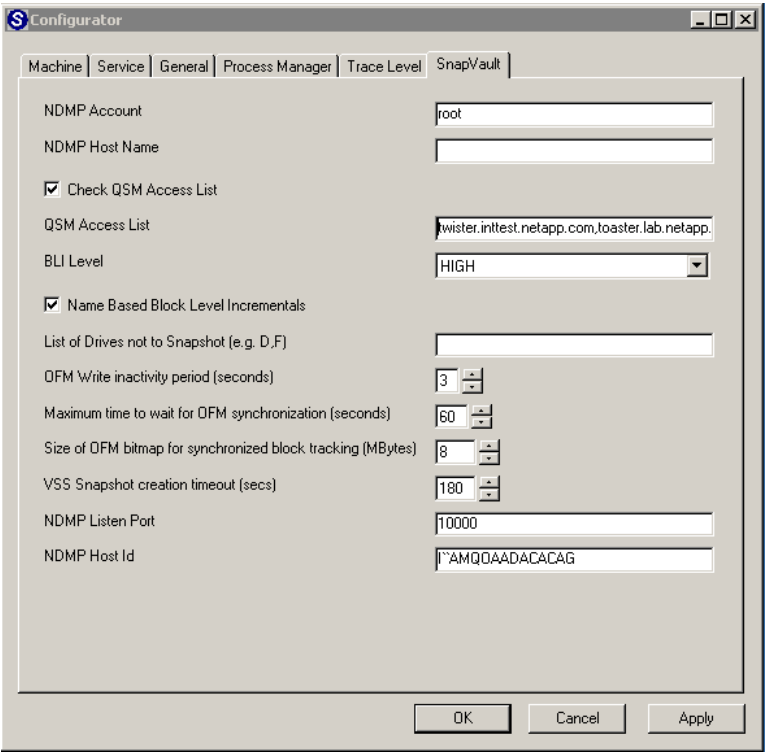
OFM supports one active snapshot per disk volume letter. For example, if you try to use OFM to back up two directories on the same disk volume, one of the two directory backups will fail.

If an active snapshot is encountered during an attempted backup, OFM fails.

Note

OFM requires a quiescent period of process inactivity to synchronize and take a snapshot of the target drive. Without this quiescent period, OFM will not initiate a snapshot. An OFM failure can result in a blank backup.

To configure OFM, complete the following steps.

Step	Action
1	Click the SnapVault tab, as shown in the following window. 
2	Click the up and down arrows to change the “OFM Write inactivity period (seconds)” value. You can select between 1 and 60 seconds. The default value is 3 seconds. Result: OFM waits this amount of time, in seconds, for the write inactivity required.

Step	Action
3	Click the up and down arrows to change the “Maximum time to wait for OFM synchronization (seconds)” value. You can set the time between 1 and 60 seconds. The default value is 60 seconds. The synchronization timeout is the maximum wait time that is allowed for OFM to find a period of write inactivity before the wait is ended.
4	Click the up and down arrows to change the “Size of OFM bitmap for synchronized block tracking (MBytes)” value. You can set the size between 1 and 50 MB. The default value is 8 MB. Result: This sets the maximum amount of memory in MB that OFM uses to track changed blocks during the backup process.

Setting the VSS snapshot timeout parameter on Windows 2003

Certain conditions must be met before the Open Systems SnapVault agent can acquire a VSS snapshot. You can set the amount of time (snapshot timeout) that the agent waits until it retries a VSS snapshot if the conditions are not right at the time. Setting this parameter avoids unacceptably long waiting periods.

To set the VSS snapshot timeout parameter on Windows 2003, complete the following steps.

Step	Action
1	Click the SnapVault tab.
2	Click the up and down arrows to change the “VSS Snapshot creation timeout (secs)” value. You can set a time between 1 and 180 seconds. The default value is 180 seconds.
3	Click OK.

Backing up and restoring Windows System State data

Creating and using System State backups

You can add backups of Windows System State data to existing Open Systems SnapVault backup schedules and use the backups to restore a system to an earlier state, for example if an Active Directory entry is accidentally deleted. You can also use Open Systems SnapVault System State data backup in conjunction with complete file system backups as part of a disaster recovery plan. Creating and using System State data backups include the following activities:

- ◆ [Adding System State data backup](#)
- ◆ [Restoring System State data from a backup](#)
- ◆ [Restoring System State data from a backup and marking it primary](#)
- ◆ [Preparing disaster recovery backups](#)
- ◆ [Using disaster recovery backups](#)

Because you are backing and restoring Windows System State data, including both registry information and domain information, there are a number of potential issues beyond the basic restoring of data.

For example, if you restore registry data from one system to a different system, the restored registry entries might not be the correct entries for the new system. Performance might be degraded or the system might not be functional. See the Microsoft Knowledge Base for information on such issues.

Primary, authoritative and non-authoritative restores

Two components of the Windows System State data involve functions normally coordinated over multiple systems: Active Directory and SYSVOL (or the File Replication Service). Inherent to these distributed system is their interaction with Active Directory and SYSVOL functions on other systems in a domain/forest. The Active Directory on a restored system can have its authority option set to authoritative or non-authoritative. The SYSVOL authority option can be authoritative, non-authoritative or primary.

Windows does not restrict any combinations of Active Directory and SYSVOL authority options, for example a system can have an authoritative Active Directory and non-authoritative SYSVOL. However, Microsoft recommends that when System State data is restored:

- ◆ A primary restore should only be used when all domain controllers have been lost and the domain is being completely recreated.

- ◆ Because of interactions between Active Directory and SYSVOL, they should have matching authority.

These two points result in three combinations of restore scenario, SYSVOL authority and Active Directory authority as shown in the following table:

Scenario	SYSVOL Authority	Active Directory Authority
Recreating the first or only domain controller	primary	authoritative
Performing a non-authoritative restore of System State data or as a part of disaster recovery	non-authoritative	non-authoritative
Performing an authoritative restore of System State data or as a part of disaster recovery	authoritative	authoritative

Active Directory restores performed by Open Systems SnapVault can only be non-authoritative, but you can use the Windows utility `ntdsutil` to change the authority. SYSVOL restores performed by Open Systems SnapVault can be primary, authoritative or non-authoritative by using the `snapvault restore` command secondary path options `SystemStatePrimary`, `SystemStateAuthoritative` or `SystemState`, respectively.

Disaster Recovery Planning

As part of your disaster recovery planning, consider the Active Directory and SYSVOL authority status of each system in the domain and use it to determine in what order to restore systems, and what authority settings to use when they are restored. Take in account the following:

- ◆ A non-authoritative system cannot become the domain controller until the file replication service permits. This means a non-authoritative system cannot become the domain controller until it contacts another system with a working file replication service.
- ◆ A restored domain controller assigned certain FMSO Active Directory roles will not function as the domain controller until it has replicated with another domain controller.

For example, if the restored domain controller has the RID Master role, it must contact another domain controller with which it is set to replicate before the restored domain controller will function as the domain controller.

Also review the Microsoft Knowledge Base for additional issues.

Adding System State data backup

Note

On Windows 2000 systems, before starting System State data backups, make sure the system has recent Windows Service Packs installed. You can have problems with restored systems if the backed-up system was running an older version of the operating system.

To initiate a System State data backup, and to add System State data backup to an existing Open Systems SnapVault backup schedule, complete the following step.

Step	Action
1	In the filer console of the SnapVault secondary system, enter the following command: <pre>snapvault start -S prim_host:SystemState sec_host:/vol/sec_vol/sec_tree</pre> Note The keyword systemstate is case independent. Example: <pre>snapvault start -S melzhost:SystemState sv_secondary:/vol/sv_vol/tree_melz</pre>

Note

System State data backups of domain controllers are only valid for the configured tombstone lifetime setting for the enterprise. The default tombstone lifetime is 60 days.

Boot files and system files are backed up even when they are on different volumes.

Subsequent backups use block incremental backups.

Restoring System State data from a backup

Use this procedure to restore the System State data, unless all domain controllers are being recreated, and this is the first domain controller to be restored. In that case use the procedure “[Restoring System State data from a backup and marking it primary](#)” on page 61.

To restore the System State data from a backup, complete the following steps.

Step	Action
1	If the machine is a domain controller, reboot it into Directory Services Restore Mode. (You can enter the Directory Services Restore Mode by holding down the Ctrl key when the machine is booting, and then pressing the F8 key at the startup menu.)
2	On the primary, enter the following command: <pre>snapvault restore -S sec_host:/vol/sec_vol/sec_tree SystemState</pre> Note_____ The keyword systemstate is case independent. _____ Example: <pre>snapvault restore -S sv_secondary:/vol/sv_vol/tree_melz SystemState</pre>
3	Restored Active Directory information is marked as non-authoritative. When a domain controller with non-authoritative entries reconnects to the domain, replication services update those entries with authoritative values. To mark any or all of the restored entries as authoritative, use the Microsoft ntdsutil tool. Otherwise skip to the next step.
4	Reboot.

Restoring System State data from a backup and marking it primary

Use this procedure to restore the System State data for the first domain controller after all domain controllers have been lost. Do not use this procedure if there are still functioning domain controllers. To restore the System State data from a backup, complete the following steps.

Step	Action
1	If the machine is a domain controller, reboot it into Directory Services Restore Mode. (You can enter the Directory Services Restore Mode by holding down the Ctrl key when the machine is booting, and then pressing the F8 key at the startup menu.)
2	In the primary system, enter the following command: <pre>snapvault restore -S sec_host:/vol/sec_vol/sec_tree SystemStatePrimary</pre> Note_____ The keyword systemstateprimary is case independent. _____ Example: <pre>snapvault restore -S sv_secondary:/vol/sv_vol/tree_melz SystemStatePrimary</pre>
3	Reboot.

Preparing disaster recovery backups

You can use System State data backups as part of a disaster recovery plan.

To create a backup for use as part of a disaster recovery plan, complete the following steps.

Step	Action
1	Back up the entire system drive.
2	If a computer utility partition exists, and is accessible as part of a file system, back up the partition.

Step	Action
3	In the filer console of the SnapVault secondary system, enter the following command: <pre>snapvault start -S prim_host:SystemState sec_host:/vol/sec_vol/sec_tree</pre> Note_____ The keyword systemstate is case independent. _____ Example: <pre>snapvault start -S melzhost:SystemState sv_secondary:/vol/sv_vol/tree_melz</pre>

Note_____

Open Systems SnapVault files are not backed up, because they are modified during the backup.

This procedure is designed to back up the operating system and its state. The procedure does not reliably back up all application data. Review your application documentation for any steps necessary to back up the application and application data.

Using disaster recovery backups

Use the disaster recovery procedure to recreate a specific system. Using a System State data backup on a system that is not effectively a duplicate of the original system disables the new system. The procedure lists several areas that are required to be the same (or in the case of disk drives, same or larger), but there are also areas of potential differences such as video bus types (for example AGP bus versus PCI video bus), that might cause problems depending on the specifics of the systems. Check the *Microsoft Knowledge Base* for additional information on disaster recovery.

To rebuild a system using disaster recovery backups, complete the following steps.

Step	Action
1	Install and configure the base operating system. Note the following restrictions: ◆ Use the same operating system and service packs that were on the original system. ◆ Use the same machine name as on the original system. ◆ Use the same drive letter mappings. ◆ Make sure each drive is at least as large as the corresponding drive was when the backup was made. ◆ Format each drive with the same file system type and version as on the original system. ◆ Make sure the hardware configuration is identical to the original. Do not perform any operating system configuration tasks beyond those needed to satisfy these restrictions.
2	Install and configure Open Systems SnapVault in the same location it was installed on the original machine.
3	If the machine is a domain controller, boot into Directory Services Restore Mode.
4	Restore the system drive.
5	Restore the System State data. Choose between the procedures “Restoring System State data from a backup” on page 60 and “Restoring System State data from a backup and marking it primary” on page 61 based on the points about authoritative versus non-authoritative and primary versus non-primary restores discussed as part of the procedures.
6	Reboot.
7	Reinstall any applications not restored by steps 1 through 6.
8	Restore any application data not restored by steps 1 through 6.

Open Systems SnapVault relationships

Reusing a deleted or renamed directory name

If you delete or rename a directory that is a source of a SnapVault relationship and create another directory with the same name, the next SnapVault update transfer will fail with the following error messages:

```
Root Inode has changed
Failed to generate update inode values
```

Perform one of the following procedures to delete or recreate the Open Systems SnapVault relationship.

If the SnapVault source directory on the primary system was intentionally deleted and backups are not necessary: Complete the following steps.

Step	Action
1	Delete the backed up directory on the secondary system.
2	Release the SnapVault relationship from the Open Systems SnapVault primary system using the <code>snapvault release</code> command.

If the SnapVault source directory on the primary system was intentionally renamed: Complete the following steps.

Step	Action
1	Create a new SnapVault relationship for the renamed directory and perform a baseline transfer for the new relationship.
2	When previous backups of the original directory are no longer needed, delete the original SnapVault relationship and release that relationship from the Open Systems SnapVault primary system.

If the SnapVault source directory on the primary system was erroneously renamed: Complete the following steps.

Step	Action
1	Change the name of the directory back to its original name.
2	Continue performing update backup transfers as you did before the erroneous renaming of the directory.

Deleting and recreating Open Systems SnapVault relationships

If you use the `snapvault stop` command on the secondary to delete an Open Systems SnapVault relationship and then try to recreate the relationship, the attempt fails with an error message similar to this:

```
date and time [worker_thread_162:error]: snapvault: destination
transfer from source file to destination qtree: the qtree is not
the source for the snapmirror destination
```

Transfer aborted: the qtree is not the source for the snapmirror destination.

Instead, after stopping the relationship, but before recreating it, release the relationship on the primary system.

Follow these general steps to delete and recreate Open Systems SnapVault relationships.

Step	Action
1	On the secondary system console enter this command: snapvault stop <i>secondary_path</i>
2	On the primary system console enter this command: snapvault release <i>primary_path</i> [secondary:] <i>secondary_path</i>
3	On the secondary system console enter this command: snapvault start -S <i>primary_path</i> [secondary:] <i>secondary_path</i>

Migrating from one secondary system to another

Using the command line: Before migrating data from one secondary to another secondary, review the basics of setting up SnapVault transfers (access permission, licensing, and correct volume language for example) in the *Data*

ONTAP Online Backup and Recovery Guide. To migrate a volume that contains SnapVault destination qtrees from one secondary system to another secondary system without having to perform another baseline transfer, complete the following steps.

Step	Action
1	Ensure that you have Open Systems SnapVault baselines of the directory you are migrating. Example: In this procedure, assume a baseline of the bno:C:\500MB directory was backed up to r200-old:/vol/old_vol/bno_C_500MB.
2	Using SnapMirror, replicate the volume from the present secondary system to a volume on the new secondary system. See the SnapMirror chapter in the <i>Online Backup and Recovery Guide</i> for details about creating SnapMirror relationships. Note— This is a SnapMirror replication of a volume, not a qtree. Example: To replicate the old_vol volume from the r200-old secondary system to the new_vol volume on the r200-new secondary system, complete the following steps on the new secondary system (r200-new): 1. Create the new_vol volume. vol create new_vol 3 2. Mark the new_vol volume restricted. vol restrict new_vol 3. Transfer the old_vol volume to the new_vol volume. snapmirror initialize -S r200-old:old_vol new_vol
3	Quiesce and break the SnapMirror relationship between the old secondary system and the new secondary system. Example: To quiesce and break the SnapMirror relationship between r200-old and r200-new, complete the following steps on r200-new: 1. snapmirror quiesce new_vol 2. snapmirror break new_vol

Step	Action												
4	Check the SnapMirror status and SnapVault status on the new secondary. SnapMirror status should be Broken-off. SnapVault status should be Snapvaulted to the new volume on the new secondary system. Example: Perform the following steps from r200-new. 1. snapmirror status <table><tr><td>Source</td><td>Destination</td><td>State</td></tr><tr><td>r200-old:old_vol</td><td>r200-new:new_vol</td><td>Broken-off</td></tr></table> 2. snapvault status <table><tr><td>Source</td><td>Destination</td><td>State</td></tr><tr><td>bno:C:\500MB</td><td>r200-new:/vol/new_vol/bno_C_500MB</td><td>Snapvaulted</td></tr></table>	Source	Destination	State	r200-old:old_vol	r200-new:new_vol	Broken-off	Source	Destination	State	bno:C:\500MB	r200-new:/vol/new_vol/bno_C_500MB	Snapvaulted
Source	Destination	State											
r200-old:old_vol	r200-new:new_vol	Broken-off											
Source	Destination	State											
bno:C:\500MB	r200-new:/vol/new_vol/bno_C_500MB	Snapvaulted											
5	Confirm that SnapVault configuration information is not present on the new secondary system using the <code>snapvault status -c</code> command. Example: Perform the following step from r200-new. snapvault status -c Snapvault secondary is ON.												
6	Add SnapVault configuration information to the registry on the new secondary system using the <code>snapvault start</code> command. Note_____ This does not start a new baseline, it updates the registry. _____ Example: Perform the following step from r200-new. snapvault start -S bno:C:\500MB r200-new:/vol/new_vol/bno_C_500MB Snapvault configuration for the qtree has been set. Qtree /vol/new_vol/bno_C_500MB is already a replica.												
7	Confirm that SnapVault configuration information is present on the new secondary system using the <code>snapvault status -c</code> command. Example: Perform the following step from r200-new. snapvault status -c Snapvault secondary is ON. /vol/new_vol/bno_C_500MB source=bno:C:\500MB												

Step	Action
8	Test the new SnapVault relationship by manually updating r200-new. If you are using the command line to manage your environment, continue to the next step; otherwise, you are finished. Example: Perform the following step from r200-new. <pre>snapvault update r200-new:/vol/new_vol/bno_C_500MB</pre> Transfer started. Monitor progress with 'snapvault status' or the snapmirror log.
9	Recreate any schedules used on the old secondary system to the new secondary system and ensure access permissions are in place.

Using DataFabric Manager: To migrate a volume from one secondary to another secondary using DataFabric Manager, complete the following steps.

Step	Action
1	Complete the command line procedure before using the DataFabric Manager interface for SnapVault management of the new secondary system.
2	Ensure that the NDMP protocol is configured properly on the new secondary system, that is, ndmpd is turned on and the ndmpd password is set up.
3	Import the new relationships to the new volume and secondary system, and reestablish schedules and retention policies to the new secondary system.
4	Remove the old relationships to the old volume and old secondary system.

Migrating from one volume to another on a secondary system

Using the command line: To migrate a volume that contains SnapVault destination qtrees to another volume on the same secondary system without having to perform another baseline transfer, complete the following steps.

Step	Action
1	Ensure that you have Open Systems SnapVault baselines of the directory you are migrating. Example: In this procedure, assume a baseline of the bno:C:\500MB directory was backed up to r200:/vol/old_vol/bno_C_500MB.
2	Using SnapMirror, replicate the volume from the present volume on the secondary system to a new volume. See the SnapMirror chapter in the <i>Online Backup and Recovery Guide</i> for details about creating SnapMirror relationships. Note_____ This is a SnapMirror replication of a volume, not a qtree. Example: To replicate the old_vol volume on the r200 secondary system to the new_vol volume, complete the following steps on the secondary system (r200): 1. Create the new_vol volume. <code>vol create new_vol 3</code> 2. Mark the new_vol volume restricted. <code>vol restrict new_vol</code> 3. Transfer the old_vol volume to the new_vol volume. <code>snapmirror initialize -S r200:old_vol new_vol</code>
3	Quiesce and break the SnapMirror relationship between the old volume and the new volume. Example: To quiesce and break the SnapMirror relationship between old_vol and new_vol, complete the following steps on r200: 1. <code>snapmirror quiesce new_vol</code> 2. <code>snapmirror break new_vol</code>

Step	Action												
4	Check the SnapMirror status and SnapVault status of the new volume. SnapMirror status should be Broken-off. SnapVault status should be Snapvaulted to the new volume. Example: Perform the following steps from r200. 1. snapmirror status <table><tr><td>Source</td><td>Destination</td><td>State</td></tr><tr><td>r200:old_vol</td><td>r200:new_vol</td><td>Broken-off</td></tr></table> 2. snapvault status <table><tr><td>Source</td><td>Destination</td><td>State</td></tr><tr><td>bno:C:\500MB</td><td>r200:/vol/new_vol/bno_C_500MB</td><td>Snapvaulted</td></tr></table>	Source	Destination	State	r200:old_vol	r200:new_vol	Broken-off	Source	Destination	State	bno:C:\500MB	r200:/vol/new_vol/bno_C_500MB	Snapvaulted
Source	Destination	State											
r200:old_vol	r200:new_vol	Broken-off											
Source	Destination	State											
bno:C:\500MB	r200:/vol/new_vol/bno_C_500MB	Snapvaulted											
5	Confirm that SnapVault configuration information is not present for the new volume using the snapvault status -c command. Example: Perform the following step from r200. snapvault status -c Snapvault secondary is ON.												
6	Add SnapVault configuration information to the registry on the new volume using the snapvault start command. Note_____ This does not start a new baseline, it updates the registry. _____ Example: Perform the following step from r200. snapvault start -S bno:C:\500MB r200:/vol/new_vol/bno_C_500MB Snapvault configuration for the qtree has been set. Qtree /vol/new_vol/bno_C_500MB is already a replica.												
7	Confirm that SnapVault configuration information is present on the new volume using the snapvault status -c command. Example: Perform the following step from r200. snapvault status -c Snapvault secondary is ON. /vol/new_vol/bno_C_500MB source=bno:C:\500MB												

Step	Action
8	Test the new SnapVault relationship by manually updating new_vol. If you are using the command line to manage your environment, continue to the next step; otherwise, you are finished. Example: Perform the following step from r200. <pre>snapvault update r200:/vol/new_vol/bno_C_500MB</pre> Transfer started. Monitor progress with 'snapvault status' or the snapmirror log.
9	Recreate any schedules used on the old volume to the new volume and ensure access permissions are in place.

Using DataFabric Manager: To migrate from one volume to another volume using DataFabric Manager, complete the following steps.

Step	Action
1	Complete the command line procedure before using the DataFabric Manager interface for SnapVault management of the new secondary system.
2	Import the new relationships to the new volume and secondary system, and reestablish schedules and retention policies to the new secondary system.
3	Remove the old relationships to the old volume and old secondary system.

Recovering data from a partially initialized transfer

To recover data from a partially initialized transfer, complete the following steps.

Step	Action
1	Create a new snapshot on the destination volume.
2	Access the qtree data through the newly created snapshot.

Additional information

For more information

You can obtain additional information about Open Systems SnapVault from NetApp:

- ◆ For SnapVault commands and information, see the Data ONTAP *Data Protection Online Backup and Recovery Guide*.
- ◆ For Open Systems SnapVault commands and examples of establishing baselines, scheduling, and troubleshooting, see the Data ONTAP OSSV *Quick Reference Card–Windows & Solaris*, part number RC-0007-0403. You can order this quick reference card through your NetApp representative.
- ◆ For the latest information about all the Open Systems SnapVault agents, see Frequently Asked Questions (FAQ) on the NOW site.