Tivoli Storage Manager FastBack
Version 6.1.7

Installation and User's Guide

IBM

Tivoli Storage Manager FastBack
Version 6.1.7

Installation and User's Guide

IBM

Contents

Figures

Tables

Preface

This publication helps you install and use Tivoli Storage Manager FastBack.

Who should read this guide

This publication provides instructions for a user to install, configure, and use Tivoli Storage Manager FastBack.

Publications

Tivoli Storage Manager FastBack publications and other related publications are available online.

You can search publications in the Tivoli Storage Manager FastBack Information Center: http://publib.boulder.ibm.com/infocenter/tsmfbinf/v6/index.jsp

You can download PDF versions of publications from the Tivoli Storage Manager FastBack Information Center or from the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Support information

You can find support information for IBM products from various sources.

Start at the IBM Support Portal: http://www.ibm.com/support/entry/portal/. You can select the products that you are interested in and search for a wide variety of relevant information.

Getting technical training

Information about Tivoli® technical training courses is available online.

Go to the following websites to sign up for training, ask questions, and to interact with others who use IBM® storage products.

Tivoli software training and certification
> Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at http://www.ibm.com/software/tivoli/education/.

Tivoli Support Technical Exchange
> Technical experts share their knowledge and answer your questions in webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html.

Storage Management community
> Interact with others who use IBM storage management products at http://www.ibm.com/developerworks/servicemanagement/sm/index.html.

Global Tivoli User Community
> Share information and learn from other Tivoli users throughout the world at https://community.ibm.com/community/user/imwuc/home.

IBM Education Assistant
View short "how to" recordings designed to help you use IBM software products more effectively at http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp.

Searching knowledge bases

If you have a problem you can search for information in a knowledge base.

Search the Tivoli Storage Manager FastBack Information Center at http://publib.boulder.ibm.com/infocenter/tsmfbinf/v6/index.jsp.

Search the internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem.

To search multiple Internet resources for your product, go to the Tivoli Support portal at https://www.ibm.com/support/entry/portal/overview/software/tivoli/tivoli_brand_support_%28general%29 and search support for the product. From this section, you can search a variety of resources including:
- IBM technotes
- IBM downloads
- IBM Redbooks®
- Forums and newsgroups

Using IBM Support Assistant

At no additional cost, you can install on any workstation the IBM Support Assistant, a stand-alone application. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use.

The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:
- Support links
- Education links
- Ability to submit problem management reports

For more information, see the IBM Support Assistant Web site at http://www.ibm.com/software/support/isa/.

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at http://www.ibm.com/support/docview.wss?uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM Support Assistant website.

About this task

To check what fixes are available for your product, follow these steps:

Procedure

- From the IBM Support Assistant Web site at http://www.ibm.com/support/
  entry/portal/, click **Downloads**.
- Click **Search for recommended fixes**.
- Choose content filters to find fixes for your product level and operating system.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about
IBM products.

About this task

To sign up to receive notifications about IBM products, follow these steps:

Procedure

1. From the IBM Support Assistant Web site at http://www.ibm.com/support/
   entry/portal/, click **Sign in to create, manage, or view your subscriptions** in
   the **Notifications** pane.
2. Sign in using your IBM ID and password. If you do not have an ID and
   password, click **register now** and complete the registration process.
3. Click **Manage all my subscriptions** in the **Notifications** pane.
4. Click the **Subscribe** tab and then click **Tivoli**.
5. Select the products for which you want to receive notifications and click
   Continue.
6. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM subscription and
support contract and if you are authorized to submit problems to IBM.

About this task

To obtain help from IBM Software Support, complete the following steps:

Procedure

1. Ensure that you have completed the following prerequisites:
   a. Set up a subscription and support contract.
   b. Determine the business impact of your problem.
   c. Describe your problem and gather background information.
2. Follow the instructions in "Submitting the problem to IBM Software Support"
   on page xiv.

Setting up a software maintenance contract

Set up a software maintenance contract. The type of contract that you need
depends on the type of product you have.

Procedure

- For IBM distributed software products (including, but not limited to, Tivoli,
  Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere®
  products that run on Microsoft Windows or UNIX operating systems), enroll in
  IBM Passport Advantage® in one of the following ways:

- **Online:** Go to the Passport Advantage Web page at http://www.ibm.com/ software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
- **By Phone:** For the phone number to call in your country, go to the IBM Software Support Handbook Web page at http:// techsupport.services.ibm.com/guides/contacts.html and click **Contacts**.
- For server software products, you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for server software products, go to the IBM Technical support advantage Web page at http://www.ibm.com/servers/eserver/techsupport.html.

What to do next

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. For a list of telephone numbers of people who provide support for your location, go to the Software Support Handbook page at http://www.ibm.com/support/customercare/sas/f/ handbook/home.html.

Determining the business impact
When you report a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem you are reporting.

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing the problem and gathering background information
When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:
- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
- Are you using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support
You can submit the problem to IBM Software Support online or by telephone.

Online

Go to the IBM Software Support website at http://www.ibm.com/
support/entry/portal/Open_service_request/Software/
Software_support_(general). Sign in to access IBM Service Requests and
enter your information into the problem submission tool.

By telephone

For the telephone number to call in your country, go to the IBM Software
Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/
f/handbook/home.html and click **Contacts**.

Chapter 1. Tivoli Storage Manager FastBack Overview

Tivoli Storage Manager FastBack provides several functions for the purposes of backing up and restoring data with snapshots.

All data is backed up at the disk block level in full and incremental snapshots. After data is backed up, data can be restored back to a disk, or mounted as a virtual volume for an individual file restore.

Tivoli Storage Manager FastBack provides these services with three primary services: FastBack Client, FastBack Server, and FastBack Mount. FastBack Manager is the graphical user interface that you can use from a supported Windows or Linux operating system to manage the FastBack Server.

FastBack Client is a service that runs on client systems (production servers) and backs up used or changed disk blocks. FastBack Client is not an application in the sense of having a GUI or actions that you can initiate. Most activity is controlled by FastBack Server. The server hosts a repository that stores all backed up data received from the client systems. The server also initiates snapshot backups, scheduled backups, and defines all options for the backup process. You can also restore data from the server. Access to the FastBack Server is to be restricted to IT personnel.

Tivoli Storage Manager FastBack provides the following functionality:

- Full snapshots of entire disks, and incremental snapshots of entire disks. A defined set of disks to be backed up concurrently is called a client group. A client group can contain multiple disks from multiple clients.
- Advanced scheduling features of backup. Schedules are combined with client groups to create policies. A policy can contain several client groups, and several schedules. Client group, schedule, and policy creation are all controlled by using FastBack Server.
- All snapshots use Copy-On-Write. Copy-On-Write ensures snapshot integrity and accuracy while a snapshot is being taken by copying blocks from a disk just before they are to be overwritten by an application.
- (Windows only) Schedules can optionally provide Continuous Data Protection (CDP). CDP can allow for point-in-time restores by backing up changed blocks in real time, between snapshots. CDP is configured per schedule.
- Data can be restored in several ways:
  - File-level recovery.
  - Volume restore, initiated by the FastBack Server. A volume restore restores an entire volume from a specific snapshot.
  - Instant restore. An instant restore is part of FastBack Mount. Like volume restore, entire volumes are restored to existing volumes. In addition, data can be accessed near-instantaneously while an instant restore is in progress.
  - Mount a snapshot to a virtual volume through FastBack Mount. This virtual volume can be its own disk, with its own drive letter, or it can be a directory within an existing real volume. File systems on virtual volumes can be accessed and traversed as if the volume was a local disk. In this way, files can be restored individually to a separate real volume.

System components

Tivoli Storage Manager FastBack consists of the following components and services:

FastBack Server (Windows only)
> A server that is dedicated to running Tivoli Storage Manager FastBack. The FastBack Server creates block-level snapshots. The server connects directly to the storage area network (SAN) and local area network (LAN). For direct-attached storage (DAS) environments, the server moves snapshot data through the LAN. If a SAN is present, the server can be configured to move snapshot data directly through the SAN.
>
> The snapshot data is copied from the protected system, through the FastBack Server, and into the repository. The repository can be set up to use a disk, volume, or folder.
>
> The FastBack Server provides the following functions:
> - Tracking of all snapshots.
> - Transferring snapshot data through SAN or LAN.
> - Volume restoring and use of Disk Restore through FastBack Manager.
> - Security with Active Directory and built-in mechanisms.

FastBack Client
> This component backs up used or changed disk blocks.

FastBack Mount
> This service enables the mounting of any snapshot volume from the repository. You can view the snapshot locally, with read-only access, on the client system. FastBack Mount is used to restore individual files or folders (file-level restore) or volumes (instant restore). With FastBack Mount, you can complete the following tasks:
> - Verify snapshots
> - File or folder-level restore
> - Volume-level restore
> - Database verification
> - Back up to tape
> - (Linux only) Specify a local destination partition

FastBack Watchdog (Windows only)
> A service that monitors the status of the backup server. The service determines whether the server is down. If the status is down, the service sends an email to the system administrator about the server status.

FastBack DR Hub Server (Windows only)
> A server that stores the backup repository at an offsite location, is often referred as a disaster recovery site. The FastBack Server replicates the backup repository. The FastBack DR Hub Server works with an existing standard FTP server or with a Tivoli Storage Manager (TSM) server.
>
> The FastBack DR Hub Server uses a proprietary protocol with the standard FTP protocol. The FastBack Disaster Recovery protocol uses the standard FTP over SSL to ensure a secure transfer of data.
>
> The FastBack DR Hub Server can also use the TSM server as a repository. Disaster recovery on a TSM server is allowed only on random access storage pools with a device type of DISK or FILE. A disaster recovery

repository on a sequential storage pool is not supported. Also, ensure, that on a TSM server, the data is not migrated from sequential storage pool to a TAPE storage pool.

The FastBack DR Hub Server is sometimes called the FastBack Disaster Recovery Hub Server, the FastBack Disaster Recovery Hub, and the DR Hub Server.

FastBack Reporting (Windows only)
A service that summarizes how repositories, policies, and snapshots use resources in your network environment. FastBack Reporting uses the Tivoli Common Reporting tool to run and view reports.

In addition, Tivoli Storage Manager FastBack provides the following interfaces:

FastBack Manager
FastBack Manager is a stand-alone graphical user interface. You can use the FastBack Manager to initiate various tasks, such as:
- Managing the snapshot repository
- Scheduling snapshots
- Determining the result of backup jobs
- Monitoring which snapshots are completed, in-process, and pending
- Performing data recovery
- Scheduling bandwidth throttling of the Data Recovery network between the FastBack Server and Tivoli Storage Manager server
- Monitoring Tivoli Storage Manager FastBack system events
- Configuring and managing user group privileges and security authentications for specific users

Multiple remote FastBack Manager sessions can be active simultaneously so different users can simultaneously access the FastBack Server.

Central Control Station (Windows only)
A Microsoft Foundation Class (MFC) graphical user interface that provides a view of status files that are stored for the FastBack DR Hub Server database. When at the disaster recovery location, you can use Central Control Station with FastBack Manager to administer all remote FastBack Servers.

Administrative Command Line
The command line interface that is used to access Tivoli Storage Manager FastBack functions. The Administrative Command Line is sometimes called the FastBack Shell.

The following figure shows the high-level architecture of Tivoli Storage Manager FastBack in the branches:
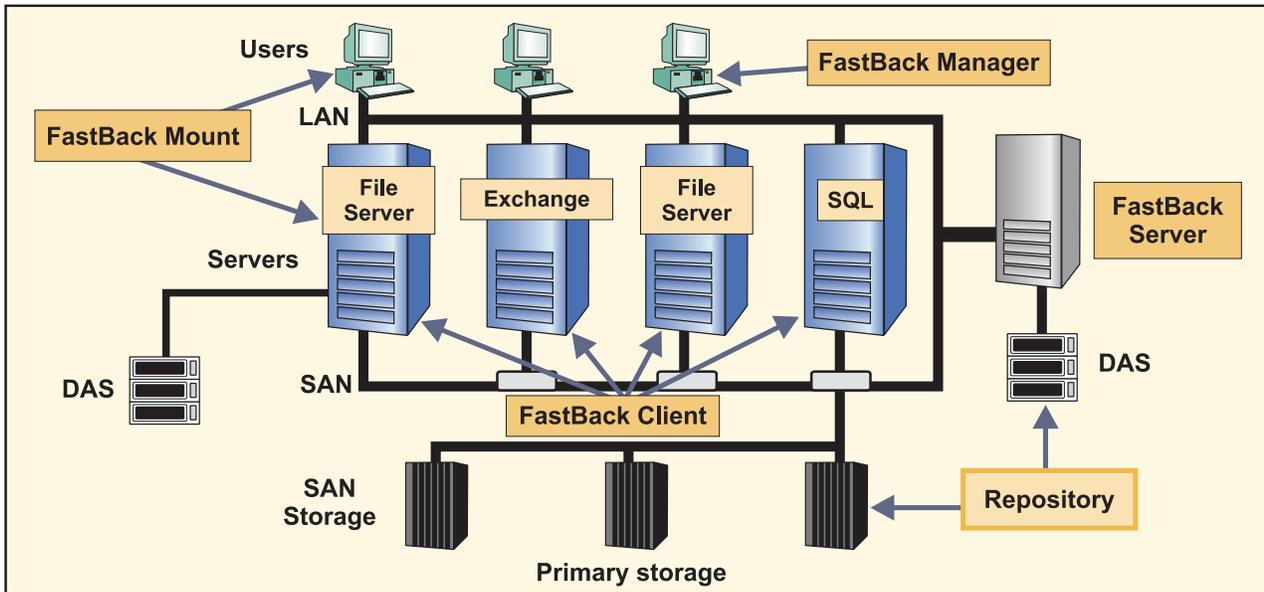
Figure 1. Tivoli Storage Manager FastBack high-level branch architecture

The following figure shows the global architecture for Tivoli Storage Manager FastBack:
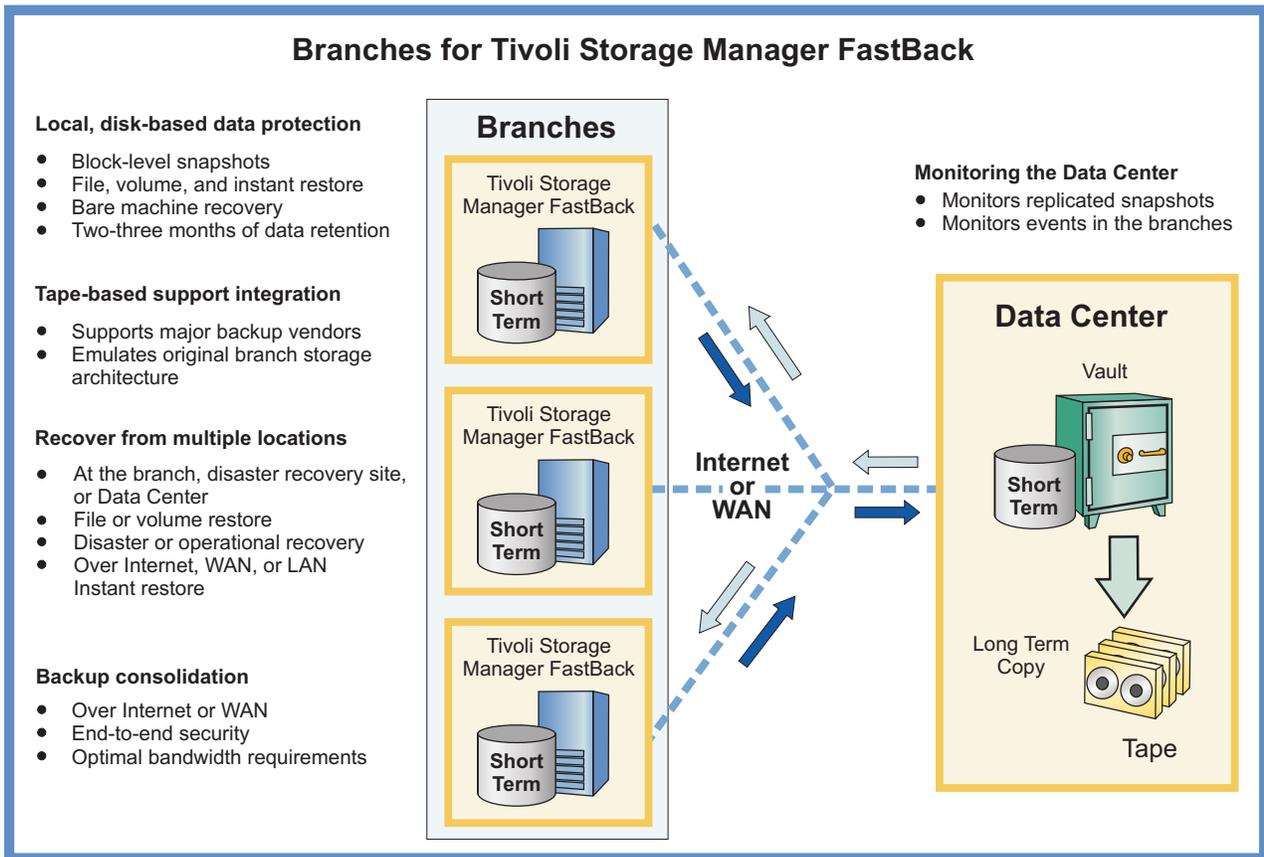
Figure 2. Tivoli Storage Manager FastBack global architecture

Data deduplication

Data deduplication is a method of eliminating redundant data in sequential-access disk (FILE) primary, copy, and active-data storage pools. One unique instance of the data is retained on storage media, and redundant data is replaced with a pointer to the unique data copy. The goal of deduplication is to reduce the overall amount of time that is required to retrieve data. This goal is achieved by storing more data on volumes and in folders, rather than on tape.

FastBack data deduplication is a service that runs on the FastBack Server system. When you use data deduplication, extra disk I/O and processor resources are required. Data deduplication is only available for Tivoli Storage Manager FastBack version 6.1.0 (or later). For more information about the hardware requirements related to data deduplication, see "Hardware requirements" on page 26.

To start FastBack data deduplication, you must identify a repository (either a volume or folder) as the data deduplication repository. This repository must be on a local volume or folder and cannot be on remote storage. Only one repository can be identified for data deduplication. If you are going to identify a repository as the data deduplication repository, you must complete this step when you create the repository. Data deduplication repositories and non-data deduplication repositories are mutually exclusive. Therefore, you cannot have a data deduplication repository and a non-data deduplication repository on the same FastBack Server. In addition, you cannot migrate from data deduplication repositories to non-data deduplication repositories, nor can you migrate from non-data deduplication repositories to data deduplication repositories. For more information about identifying a repository for data deduplication, see "Creating repositories" on page 97.

Note: When using Tivoli Storage Manager FastBack, FastBack data deduplication might be called *dedupe*. If you see the term *dedupe*, the term is a reference to data deduplication.

Note: Continuous Data Protection is not supported on repositories used with data deduplication.

Using data deduplication in a wide area network

Tivoli Storage Manager FastBack provides deduplication for replicated data that is sent between the FastBack Server and the FastBack Disaster Recovery Hub server. The deduplicated data is sent to the FastBack Disaster Recovery Hub server repository over wide area network (WAN) connections. The Tivoli Storage Manager server is then used as the storage target for the replicated data.

Without deduplication, replication of data from a Tivoli Storage Manager FastBack server over the wide area network is done through FTP sessions. The data is stored on the Tivoli Storage Manager FastBack DR Hub server in Tivoli Storage Manager FastBack format. However, when deduplicated data is replicated over the wide area network with Tivoli Storage Manager FastBack, the data is sent through the Tivoli Storage Manager API. The data is stored in Tivoli Storage Manager format within a storage pool.

The Tivoli Storage Manager FastBack file system that uses Tivoli Storage Manager FastBack storage for data deduplication is called the Tivoli Storage Manager file system. The Tivoli Storage Manager file system functions in a manner similar to the existing Tivoli Storage Manager FastBack FTP file system. However, in this Tivoli Storage Manager Disaster Recovery process, the FastBack Server replicates

the repository data to Tivoli Storage Manager server storage instead of to an FTP server. This task is accomplished by using the Tivoli Storage Manager API instead of Win32 calls on the local file system.

As shown in Figure 3 on page 7, the following events occur during Disaster Recovery processing:

1. FastBack Disaster Recovery Hub server connects to the Tivoli Storage Manager server to organize the replicated data through the Tivoli Storage Manager API.

2. FastBack Mount, Tivoli Storage Manager FastBack Central Control Station, and Tivoli Storage Manager FastBack for Bare Machine Recovery use the Tivoli Storage Manager API to access the replicated data on the FastBack Disaster Recovery Hub server. This server connects to the Tivoli Storage Manager server.

3. FastBack Server connects to the Tivoli Storage Manager server as a node and copies the data into a file space.

4. The Disaster Recovery process can be configured to connect regularly with this server node or to connect with a different node. The different node is called the virtual node and is specified with the asnodename option.

5. The Disaster Recovery process can be configured to schedule bandwidth throttling of the DR traffic between the FastBack Server and the FastBack DR Hub Server. Bandwidth throttling transfers data at a rate that does not exceed the maximum bandwidth of the network.

6. The FastBack Disaster Recovery Hub server accesses the Disaster Recovery Data with the virtual node of the branch that is being accessed. This access occurs because a node cannot view data that is defined to a different node.

   The node defined for the FastBack Disaster Recovery Hub server has permissions to connect as all the nodes that participate in Disaster Recovery operations. The FastBack DR Hub Server sends the node name and password each time it connects to a Tivoli Storage Manager server. This credential method allows multiple FastBack Servers to connect by using the same node credentials. A node can also be registered on the Tivoli Storage Manager server for recovery purposes. Such registration enables the Tivoli Storage Manager FastBack for Bare Machine Recovery process to use those same credentials when connecting to the Tivoli Storage Manager server. The availability of using the regular node or the virtual node provides flexibility, security, and separation between branches.

See "Configuring Tivoli Storage Manager FastBack Wide Area Network deduplication" on page 196 for detailed instructions.
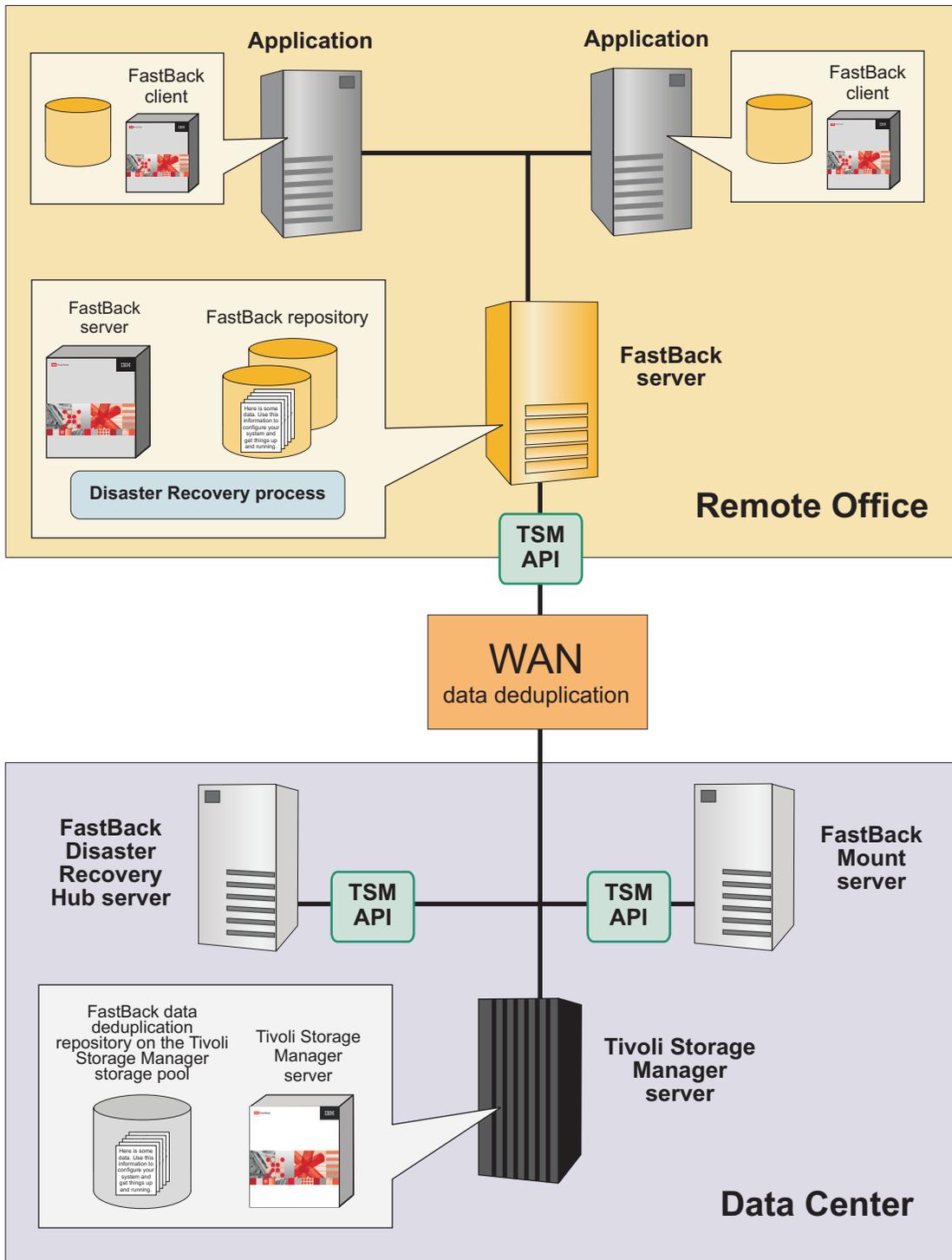
Figure 3. WAN data deduplication

New in Tivoli Storage Manager FastBack version 6.1.7

Tivoli Storage Manager FastBack is updated for version 6.1.7 and includes new enhancements and features.

Throughout this publication, technical updates since the previous editions are marked with a vertical bar (|) in the left margin.

The following features are new for Tivoli Storage Manager FastBack in version 6.1.7:

Bandwidth Throttling

Tivoli Storage Manager FastBack provides control for bandwidth throttling to limit network usage for data transfers to the FastBack Disaster Recovery Hub Server.

New and Changed CLI commands

Tivoli Storage Manager FastBack provides the alerts view option and three new CLI commands. They display information for Heart Beat alert email, client status, repository space, and server version.

Chapter 2. Planning

This release of Tivoli Storage Manager FastBack is supported on a limited number of operating systems.

Before beginning the Tivoli Storage Manager FastBack installation, verify that your system is running a supported operating system, and that you meet all hardware and software requirements.

Tivoli Storage Manager FastBack supports any disk configuration that is supported by the hardware and operating system. The disk configuration includes multi-path device drivers. The following device drivers were tested as part of the Tivoli Storage Manager FastBack 6.1.0.0 release:

- SAN Volume Controller - SDD
- SAN Volume Controller - SDD (MPIO)
- DS3400 RDAC
- DS8000® SDD

Problems with drivers that were not tested are treated as technical support issues. Technical support works with third-party vendors to resolve these issues. Multi-path device driver issues are not anticipated. However, if the controller is not on the list of controllers that were tested as part of the Tivoli Storage Manager FastBack 6.1.0.0 release, a Proof of Concept can help ensure controller compatibility with Tivoli Storage Manager FastBack.

Operating systems

Before you install, make sure that you use a supported operating system.

FastBack Server (Windows only)

The following table provides details about operating systems that are supported for FastBack Server.

Table 1. Operating systems for FastBack Server

Operating system and supported release	Support details
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors. • Does not support Microsoft Windows 2003 servers on hardware that works under UEFI.

Table 1. Operating systems for FastBack Server (continued)

Operating system and supported release	Support details
Microsoft Windows 2008 32-bit for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors.
Microsoft Windows 2008 R2 Foundation, Standard, Storage, or Enterprise Edition only	• Supports the x64 (64 bit) instruction set architecture only. • Boot and Windows operating system partitions must be formatted in NTFS.
Microsoft Windows 7 Professional and Ultimate Editions	• Supports the x86 (32 bit) and x64 (64 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.

Tivoli Storage Manager FastBack supports a single repository volume or folder to a maximum size of 16 TB provided GUID partition table (GPT) disks or network-attached storage (NAS) volumes are attached to the FastBack Server. This limit applies to both data deduplication and non-data deduplication repositories.

Note: The required repository size is three times the data size the server is backing up. The preferred repository size is five times the original data size.

FastBack Client

The following table provides details about operating systems that are supported for FastBack Client.

Table 2. Operating systems for FastBack Client

Operating system and supported release	Support details
Microsoft Windows 2000, Service Pack 3 or later for the following servers: • Standard Server • Advanced Server • Professional Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.

Table 2. Operating systems for FastBack Client (continued)

Operating system and supported release	Support details
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows 2003 64-bit Edition	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors.
Microsoft Windows 2008, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit), x64 (AMD64 and EM64T), and IA64 (Intel Itanium) instruction set architecture. • Supports 32-bit and 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows 2008, R2 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows Vista, Service Pack 1 or later: • Starter • Home Basic • Home Premium • Business • Enterprise • Ultimate	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors.

Table 2. Operating systems for FastBack Client (continued)

Operating system and supported release	Support details
Microsoft Windows 7 Professional and Ultimate Editions	• Supports the x86 (32 bit) and x64 (64 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.

Red Hat Enterprise Linux 5.2 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• The following library is required: libstdc++
	• Master boot record (MBR) and logical volume manager (LVM) are supported. For LVM, the support is only provided for volumes on a single partition where the volume occupies one set of contiguous extents. Instant restore to LVM partitions is not supported.
	• Simple volume configurations are supported. A simple volume is a volume with data stored on one partition and is allocated with contiguous extents. The simple volume must be physically on one disk, with no special software-based volume management characteristics, such as RAID 0, RAID 1, or RAID 5.
	• Advanced volume management configurations are not supported. No dynamic disk support.
	• FastBack does not support LVM partitions with multipath disks.

Table 2. Operating systems for FastBack Client (continued)

Operating system and supported release	Support details

Red Hat Enterprise Linux 5.4 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• The following library is required: libstdc++
	• Master boot record (MBR) and logical volume manager (LVM) are supported. For LVM, the support is only provided for volumes on a single partition where the volume occupies one set of contiguous extents. Instant restore to LVM partitions is not supported.
	• Simple volume configurations are supported. A simple volume is a volume with data stored on one partition and is allocated with contiguous extents. The simple volume must be physically on one disk, with no special software-based volume management characteristics, such as RAID 0, RAID 1, or RAID 5.
	• Advanced volume management configurations are not supported. No dynamic disk support.
	• FastBack does not support LVM partitions with multipath disks.

Table 2. Operating systems for FastBack Client (continued)

Operating system and supported release	Support details

Red Hat Enterprise Linux 5.8 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	 • Supports the x86 (32 bit) instruction set architecture.
	 • Supports 32-bit and 64-bit processors.
	 • SCSI and SATA disks are supported.
	 • IDE devices are supported.
	 • The following kernels are supported:
	   – RedHat-i386: 2.6.18-308.e15.i686 and 2.6.18-308.e15.i686 PAE
	   – RedHat-x86_64: 2.6.18-308.el5-x86_64
	 • The following library is required: libstdc++
	 • Master boot record (MBR) and logical volume manager (LVM) are supported. For LVM, the support is only provided for volumes on a single partition where the volume occupies one set of contiguous extents. Instant restore to LVM partitions is not supported.
	 • Simple volume configurations are supported. A simple volume is a volume with data stored on one partition and is allocated with contiguous extents. The simple volume must be physically on one disk, with no special software-based volume management characteristics, such as RAID 0, RAID 1, or RAID 5.
	 • Advanced volume management configurations are not supported. No dynamic disk support.
	 • FastBack does not support LVM partitions with multipath disks.

Table 2. Operating systems for FastBack Client (continued)

Operating system and supported release	Support details

Red Hat Enterprise Linux 6.3 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.32-279.e16.i686 and 2.6.32-279.e16.i686 PAE
	  – RedHat-x86_64: 2.6.32-279.el6-x86_64
	• The following library is required: libstdc++
	• Master boot record (MBR) and logical volume manager (LVM) are supported. For LVM, the support is only provided for volumes on a single partition where the volume occupies one set of contiguous extents. Instant restore to LVM partitions is not supported.
	• Simple volume configurations are supported. A simple volume is a volume with data stored on one partition and is allocated with contiguous extents. The simple volume must be physically on one disk, with no special software-based volume management characteristics, such as RAID 0, RAID 1, or RAID 5.
	• Advanced volume management configurations are not supported. No dynamic disk support.
	• FastBack does not support LVM partitions with multipath disks.

Table 2. Operating systems for FastBack Client (continued)

Operating system and supported release	Support details

SUSE Linux Enterprise Server 10, Service Pack 2	• Operating system partitions must be formatted in EXT2, EXT3, and Reiser file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – SUSE-i386: 2.6.16.60-0.21default, 2.6.16.60-0.21smp, and 2.6.16.60-0.21bigsmp
	  – SUSE-x86_64: 2.6.16.60-0.21default and 2.6.16.60-0.21smp
	For all kernel versions, auto mount is not supported.
	• Master boot record (MBR) and logical volume manager (LVM) are supported. For LVM, the support is only provided for volumes on a single partition where the volume occupies one set of contiguous extents. Instant restore to LVM partitions is not supported.
	• Simple volume configurations are supported. A simple volume is a volume with data stored on one partition and is allocated with contiguous extents. The simple volume must be physically on one disk, with no special software-based volume management characteristics, such as RAID 0, RAID 1, or RAID 5.
	• Advanced volume management configurations are not supported. No dynamic disk support.
	• FastBack does not support LVM partitions with multipath disks.

SUSE Linux Enterprise Server 11, Service Pack 2	• Operating system partitions must be formatted in EXT2, EXT3, and Reiser file systems. • SCSI and SATA disks are supported. IDE devices are supported. • The following kernels are supported: – SUSE-x86_64: 3.0.13-x.y - default For all kernel versions, auto mount is not supported. • Master boot record (MBR) and logical volume manager (LVM) are supported. For LVM, the support is only provided for volumes on a single partition where the volume occupies one set of contiguous extents. Instant restore to LVM partitions is not supported. • Simple volume configurations are supported. A simple volume is a volume with data stored on one partition and is allocated with contiguous extents. The simple volume is to exist on one disk, with no special software-based volume management characteristics, such as RAID 0, RAID 1, or RAID 5. • Advanced volume management configurations are not supported. No dynamic disk support. • FastBack does not support LVM partitions with multi-path disks.

A maximum of 40 clients are allowed to connect to a FastBack Server, and a single FastBack Server protects production data up to a maximum size of 8 TB. As with prior releases, the maximum size of a "repository on disk" repository object is 2 TB. The disk must not be equal to or greater than 2 TB in size.

Note:

- (Windows only) Support is not provided for applications that use SCSI Pass Through Interface (SPTI) or SCSI Pass Through Direct (SPTD) for processing read and write operations. You cannot back up or use instant restore while applications that use SPTI or SPTD are running. If you try to back up or use instant restore while applications that use SPTI or SPTD are running, it might look like the backup or instant restore was completed, but the data can be corrupted.
- (Red Hat Enterprise Linux 6.3 Server only) The Ext 4 file system is now the default file system for Red Hat Enterprise Linux 6.3 Server. However, you must ensure that all partitions are formatted in EXT2 and EXT3 file systems.

Administrative Command Line

The following table provides details about operating systems that are supported for Administrative Command Line.

Table 3. Operating systems for Administrative Command Line

Operating system and supported release	Support details
Microsoft Windows 2000, Service Pack 3 or later for the following servers: • Standard Server • Advanced Server • Professional Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows 2003 64-bit Edition	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors.

Table 3. Operating systems for Administrative Command Line (continued)

Operating system and supported release	Support details
Microsoft Windows 2008, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit), x64 (AMD64 and EM64T), and IA64 (Intel Itanium) instruction set architecture. • Supports 32-bit and 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows 2008, R2 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows Vista, Service Pack 1 or later: • Starter • Home Basic • Home Premium • Business • Enterprise • Ultimate	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors.

Red Hat Enterprise Linux 5.2 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• The following library is required: libstdc++
	• For all kernel versions, auto mount is not supported.

Table 3. Operating systems for Administrative Command Line (continued)

Operating system and supported release	Support details

Red Hat Enterprise Linux 5.4 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• The following library is required: libstdc++
	• For all kernel versions, auto mount is not supported.

SUSE Linux Enterprise Server 10, Service Pack 2	• Operating system partitions must be formatted in EXT2, EXT3, and Reiser file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – SUSE-i386: 2.6.16.60-0.21default, 2.6.16.60-0.21smp, and 2.6.16.60-0.21bigsmp
	  – SUSE-x86_64: 2.6.16.60-0.21default and 2.6.16.60-0.21smp
	
	For all kernel versions, auto mount is not supported.

FastBack Mount

The following table provides details about operating systems that are supported for FastBack Mount.

Table 4. Operating systems for FastBack Mount

Operating system and supported release	Support details
Microsoft Windows 2000, Service Pack 3 or later for the following servers: • Standard Server • Advanced Server • Professional Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture. • Supports 32-bit and 64-bit processors.

Table 4. Operating systems for FastBack Mount (continued)

Operating system and supported release	Support details
Microsoft Windows 2003 64-bit Edition	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors.
Microsoft Windows 2008, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit), x64 (AMD64 and EM64T), and IA64 (Intel Itanium) instruction set architecture. • Supports 32-bit and 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows 2008, R2 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows Vista, Service Pack 1 or later: • Starter • Home Basic • Home Premium • Business • Enterprise • Ultimate	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors.

Table 4. Operating systems for FastBack Mount (continued)

Operating system and supported release	Support details

Red Hat Enterprise Linux 5.2 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• Perl version 5 on Linux systems
	• **mdadm** tool for managing Linux Software RAID arrays
	• iSCSI Initiator for Linux package iscsi-initiator-utils-6.2.0.868-0.7.el5
	• Secure Shell (SSH) client for Linux

Red Hat Enterprise Linux 5.4 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• Perl version 5 on Linux systems
	• **mdadm** tool for managing Linux Software RAID arrays
	• iSCSI Initiator for Linux package iscsi-initiator-utils-6.2.0.868-0.7.el5
	• Secure Shell (SSH) client for Linux

Table 4. Operating systems for FastBack Mount (continued)

Operating system and supported release	Support details

SUSE Linux Enterprise Server 10, Service Pack 2	• Operating system partitions must be formatted in EXT2, EXT3, and Reiser file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – SUSE-i386: 2.6.16.60-0.21default, 2.6.16.60-0.21smp, and 2.6.16.60-0.21bigsmp
	  – SUSE-x86_64: 2.6.16.60-0.21default and 2.6.16.60-0.21smp
	For all kernel versions, auto mount is not supported.
	• Perl version 5 on Linux systems
	• **mdadm** tool for managing Linux Software RAID arrays
	• iSCSI Initiator for Linux
	• Secure Shell (SSH) client for Linux

You can use instant restore, part of FastBack Mount, only with mounted volumes.

Note: (Windows only) Support is not provided for applications that use SCSI Pass Through Interface (SPTI) or SCSI Pass Through Direct (SPTD) for processing read and write operations. You cannot back up or use instant restore while applications that use SPTI or SPTD are running. If you try to back up or use instant restore while applications that use SPTI or SPTD are running, it might look like the backup or instant restore was completed, but the data can be corrupted.

FastBack Manager

The following table provides details about operating systems that are supported for FastBack Manager.

Table 5. Operating systems for FastBack Manager

Operating system and supported release	Support details
Microsoft Windows 2000, Service Pack 3 or later for the following servers: • Standard Server • Advanced Server • Professional Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.

Table 5. Operating systems for FastBack Manager (continued)

Operating system and supported release	Support details
Microsoft Windows 2008 32-bit for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows 2008, R2 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture. • Supports 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors.

Red Hat Enterprise Linux 5.2 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• The following library is required: libstdc++

Table 5. Operating systems for FastBack Manager (continued)

Operating system and supported release	Support details

Red Hat Enterprise Linux 5.4 Server	• Operating system partitions must be formatted in EXT2 and EXT3 file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE
	  – RedHat-x86_64: 2.6.18-92.el5-x86_64
	• The following library is required: libstdc++

SUSE Linux Enterprise Server 10, Service Pack 2	• Operating system partitions must be formatted in EXT2, EXT3, and Reiser file systems.
	• Supports the x86 (32 bit) instruction set architecture.
	• Supports 32-bit and 64-bit processors.
	• SCSI and SATA disks are supported.
	• IDE devices are supported.
	• The following kernels are supported:
	  – SUSE-i386: 2.6.16.60-0.21default, 2.6.16.60-0.21smp, and 2.6.16.60-0.21bigsmp
	  – SUSE-x86_64: 2.6.16.60-0.21default and 2.6.16.60-0.21smp

FastBack DR Hub Server (Windows only)

The following table provides details about operating systems that are supported for FastBack DR Hub Server, including FastBack Disaster Recovery and Central Control Station.

Table 6. Operating systems for FastBack DR Hub Server, including FastBack Disaster Recovery and Central Control Station

Operating system and supported release	Support details
Microsoft Windows 2000 Standard Server, Service Pack 3 or later	Boot and Windows operating system partitions must be formatted in NTFS.
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.

Table 6. Operating systems for FastBack DR Hub Server, including FastBack Disaster Recovery and Central Control Station (continued)

Operating system and supported release	Support details
Microsoft Windows 2008: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors. • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/ default.aspx?scid=kb;EN-US;970770 . Download the fix that is associated with this knowledge base article.
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit processors.

The following table provides details about operating systems that are supported for FastBack Disaster Recovery with File Transfer Protocol.

Table 7. Operating systems for FastBack Disaster Recovery with File Transfer Protocol

Operating system and supported release	Support details
Microsoft Windows 2003, Service Pack 1 with fix KB931319	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.
Microsoft Windows 2003, Service Pack 2	• Boot and Windows operating system partitions must be formatted in NTFS. • Supports the x86 (32 bit) instruction set architecture. • Supports 32-bit and 64-bit processors.

FastBack Reporting (Windows only)

Because FastBack Reporting runs on the same system as the FastBack Server, the operating system requirements for FastBack Reporting are the same as the operating system requirements for FastBack Server. For more information, see "FastBack Server (Windows only)" on page 9.

Restriction: IBM Tivoli Common Reporting does not support Windows Server 2008 R2. For information about how to use FastBack Reporting on Windows Server 2008 R2, see the Setting up FastBack Reporting on Windows 2008 R2 technote http://www.ibm.com/support/docview.wss?uid=swg21569062.

Support for virtual machines and virtualization

When you run Tivoli Storage Manager FastBack software on virtual machines and through virtualization, the guest system must run an operating system that is

supported by the Tivoli Storage Manager FastBack component. For example, the guest system where the FastBack Server is installed must run one of the supported operating systems for FastBack Server.

The following list summarizes support for virtual machines and virtualization:

VMware ESX guest
> Tivoli Storage Manager FastBack products and components are supported for backup and recovery within the VMware ESX virtual guest. When you add a repository by using VMware ESX virtual guest, use either a folder or volume for the repository. Other types of repositories cannot be added when you use VMware ESX virtual guest.

Microsoft Hyper-V virtual guest
> Tivoli Storage Manager FastBack products and components are supported for backup and recovery within the Microsoft Hyper-V virtual guest. Backup of the Hyper-V virtual machines from the parent partition with MicrosoftVolume Shadow Copy Services (VSS) is not supported. When you add a repository with Microsoft Hyper-V virtual guest, use either a folder or volume for the repository. Other types of repositories cannot be added when you use Microsoft Hyper-V virtual guest.

Hardware requirements

A local FastBack Server is required. If you do not want to use a separate server for backup, a FastBack Server needs to be collocated on an application server.

Hardware requirements vary and depend on the following items:
- Number of protected servers
- Number of protected volumes
- Data set sizes
- LAN and SAN connectivity
- Repository disk throughput

FastBack Server requirements (Windows only)

The following table describes the hardware requirements that are needed to install a FastBack Server. The FastBack Server is sometimes called a backup server.

Table 8. Hardware requirements for FastBack Server

Component	Minimal requirement	Preferred
System	3-GHz Dual Intel Pentium D processor or compatible	For a FastBack Server with data deduplication enabled, the preferred requirement is a 4 processor cores at 3 GHz Intel Xeon or compatible.
Memory	2-GB RAM, 2-GB virtual address space	8-GB RAM, 2-GB virtual address space
Available hard disk	200 MB for 'Documents and Settings' folder **Note:** For a FastBack Server with data deduplication enabled, the minimum requirement is 1 GB.	2 GB
NIC Card	1 NIC - 100 Mbps	1 NIC - 1 Gbps

After you install the software for the FastBack Server, you need to create a repository to back up data. For more information about creating a repository, see "Creating repositories" on page 97. Before you create a repository, ensure that your repository meets the following requirements:

- In a production environment, the repository must be able to store a minimum of three times the size of the data on the server that is being backed up.
- The preferred size of the repository is five times the size of the data on the server that is being backed up.
- The minimum repository IO speed is 25 MB per second and the suggested IO speed is 40 MB per second.

Adjust the repository size according to the environment you plan to use.

If you enable FastBack data deduplication, you are limited to one FastBack Server repository.

Note: FastBack Server might fail to work with the assigned NIC. As a result, all communication to the FastBack Server service fails. This problem can occur if the **NetBIOS over TCP/IP** setting is disabled. For the NIC card used by the FastBack Server, set the NetBIOS setting to *Default* or *Enable*. If FastBack Server does not work with the NIC card, no errors are written to the log files. The FastBack Server service runs. The only indication of the problem is the following error reported to the Windows Application Event log: *FBSS7062E - FastBack Server failed to launch due to problem with a Network component.* You can correct the problem by verifying the NetBIOS setting.

FastBack Reporting requirements (Windows only)

Data deduplication information is not included in FastBack Reporting results.

The following table describes the hardware requirements that are needed to install FastBack Reporting.

Table 9. Hardware requirements for FastBack Reporting

Component	Minimal requirement	Preferred
System	3-GHz Dual Intel Pentium D processor or compatible	not applicable
Memory	3-GB RAM, 2-GB Virtual Address Space	4-GB RAM, 2-GB Virtual Address Space
Available hard disk	• 200 MB for 'Documents and Settings' folder. • An additional 30-GB free disk space (minimum). Requirements increase as historical data is gathered and stored. • At least 10-GB free space must be available in the home directory where the historical data is stored.	See Minimal requirements
NIC Card	1 NIC - 100 Mbps	1 NIC - 1 Gbps

As stated in the software requirements section, FastBack Reporting requires that you install IBM Tivoli Common Reporting, Version 1.2, Fix Pack 1. All hardware requirements for Tivoli Common Reporting, Version 1.2, Fix Pack 1 must be met before you install Tivoli Common Reporting and FastBack Reporting. For more information about Tivoli Common Reporting hardware requirements, see http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/ttcr_install.html.

Restriction: IBM Tivoli Common Reporting does not support Windows Server 2008 R2. As a result, FastBack Reporting is not available on Windows Server 2008 R2 operating systems.

FastBack Client requirements

(Windows only) The following table describes the hardware requirements that are needed to install a FastBack Client on a supported Windows operating system. In the installation wizard, the FastBack Client is also called a backup client.

Table 10. Hardware requirements for FastBack Client on a supported Windows operating system

Component	Minimal requirement	Preferred
System	733-MHz Intel Celeron or compatible	dual core 2-GHz Intel Pentium III or higher
Memory	512-MB RAM, 2-GB virtual address space	4-GB RAM, 2-GB virtual address space
Available hard disk	200 MB for 'Documents and Settings' folder	not applicable
NIC Card	1 NIC - 100 Mbps	1 NIC - 1 Gbps

(Linux only) The following table describes the hardware requirements that are needed to install a FastBack Client on a supported Linux operating system. In the installation wizard, the FastBack Client is also called a backup client.

Table 11. Hardware requirements for FastBack Client on a supported Linux operating system

Component	Minimal requirement	Preferred
System	1-GHz Intel Pentium III or higher	dual core 2-GHz Intel Pentium III or higher
Memory	1-GB RAM, 2-GB virtual address space	4-GB RAM, 2-GB virtual address space
Available hard disk	4 GB for the /opt directory	4 GB for the /opt directory
Communication protocol	TCP/IP Version 4 or Version 6 (standard with Linux shared memory protocol)	TCP/IP Version 4 or Version 6 (standard with Linux shared memory protocol)

FastBack DR Hub Server requirements (Windows only)

The following table describes the hardware requirements that are needed to install a FastBack DR Hub Server.

Table 12. Hardware requirements for FastBack DR Hub Server

Component	Minimal requirement	Preferred
System	3-GHz Dual Intel Pentium D processor or compatible	not applicable
Memory	2-GB RAM, 2-GB virtual address space	3-GB RAM, 2-GB virtual address space
Available hard disk	200 MB for 'Documents and Settings' folder	not applicable
NIC Card	1 NIC - 100 Mbps	1 NIC - 1 Gbps

There are bandwidth requirements to consider when using snapshots to back up data. The following three tables provide parameters you can use when you run snapshots.

The data capacity column relates to the amount of data that is replicated to a FastBack DR Hub Server. The required WAN/Internet upload speed column relates to the minimum acceptable upload speed for a replication operation. The T1, T2, T3, ADSL, and VDSL columns indicate whether data capacity can be transmitted at the required speed over the type of transmission standard in the maximum allowed delivery time of 120 hours.

The following table describes the bandwidth requirements that are needed for an initial, full snapshot. The following assumptions apply to these bandwidth requirements:

- Compression ratio - 2:1
- Maximum allowed delivery time - 120 hours (five days)
- Protocol usage - 10 percent

Table 13. Bandwidth requirements for an initial, full snapshot

	Data capacity (GB)	Required WAN / Internet upload speed (Kbit / s)	T1	T2	T3	ADSL	VDSL
Branch 1	50	500	Yes	Yes	Yes	Yes	Yes
Branch 2	100	1,000	Yes	Yes	Yes	Yes	Yes
Branch 3	200	2,000	No	Yes	Yes	Yes	Yes
Branch 4	300	3,000	No	Yes	Yes	Yes	Yes
Branch 5	500	5,000	No	Yes	Yes	No	Yes
Branch 6	1,000	10,000	No	No	Yes	No	Yes

The following table describes the bandwidth requirements that are needed for an initial, full snapshot with 75 percent minimal quality of service. The following assumptions apply to these bandwidth requirements:

- Compression ratio - 2:1
- Maximum allowed delivery time - 120 hours (five days)
- Protocol usage - 10 percent
- Minimal quality of service - 75 percent

Table 14. Bandwidth requirements for an initial, full snapshot with 75 percent minimal quality of service

	Data capacity (GB)	Required WAN / Internet upload speed (Kbit / s)	T1	T2	T3
Branch 1	50	800	Yes	Yes	Yes
Branch 2	100	1,600	No	Yes	Yes
Branch 3	200	3,150	No	Yes	Yes
Branch 4	300	4,750	No	Yes	Yes
Branch 5	500	8,000	No	No	Yes
Branch 6	1,000	16,000	No	No	Yes

The following table describes the bandwidth requirements that are needed for a daily incremental snapshot. The following assumptions apply to these bandwidth requirements:

- Compression ratio - 2:1
- Maximum allowed delivery time - 11 hours
- Daily incremental changes - 3 percent
- Protocol usage - 10 percent
- Minimal quality of service - 75 percent

Table 15. Bandwidth requirements for a daily incremental snapshot

	Data capacity (GB)	Incremental change capacity (GB)	Required WAN / Internet Upload Speed (Kbit/s)	T1	T2	T3
Branch 1	50	1.5	250	Yes	Yes	Yes
Branch 2	100	3	500	Yes	Yes	Yes
Branch 3	200	6	1,000	Yes	Yes	Yes
Branch 4	300	9	1,500	Yes	Yes	Yes
Branch 5	500	15	2,500	No	Yes	Yes
Branch 6	1,000	30	5,000	No	Yes	Yes

When using FastBack Disaster Recovery with Tivoli Storage Manager WAN data deduplication, performance might be impacted because of increased I/O demands. It is suggested that the processor and memory capabilities of the FastBack Disaster Recovery Hub Server be increased to accommodate data deduplication processing. See "FastBack DR Hub Server requirements (Windows only)" on page 28.

Connection and configuration hardware requirements

Before beginning the installation process, the following requirements must be met:

1. At least one of the following disks must be available for the repository: IDE, SCSI, GPT, or LUN in the SAN. Any number of LUNs in the SAN, DAS, or SCSI might be snapped or allocated to the repository at any time.

   For more information, including details about the maximum volume size, see "Add Repository wizard" on page 98.

2. For the SAN environment, assuming that the servers and the disks are already connected to the SAN switch, you must have a Fibre Channel switch with at least one available port reserved for the FastBack Server.

   You might use a Fibre Channel hub or point-to-point connection instead of a switch.

3. The system that is used for FastBack Manager must be connected to the IP network. This system might be one of the servers, a standard notebook, or a standard desktop system.

4. Use a static IP address for the network interface cards on the system used for the FastBack Server.

5. To run FastBack Mount, the system that runs FastBack Mount must have access to the repository through either the SAN (by direct access to disk) or LAN (by connecting to the shared repository on the FastBack Server.

6. When using SAN backup, all client disks must have unique signatures. If some disks have identical signatures, it is necessary for the System Admin to complete the following steps to manually change the signatures:

   a. Open the command prompt.

   b. Go to the directory that contains the Change Disk Signature .exe and .bat files. These Change Disk Signature utilities are only available from IBM support.

   c. To change the disk signatures, run the appropriate utility as follows:

      - For Microsoft Windows 7 or Vista, run the command `ChangeSignatureVista.bat <disk_number>`

      - For earlier versions of Windows, run the command `ChangeSignature.exe <disk_number>`

Dynamic disk support (Windows only)

The following types of dynamic disks are supported in a Windows environment. This list of dynamic disks assumes that the dynamic disks are created and configured with Windows Disk Administrator:

- Simple volumes
- Spanned volumes
- Mirrored volumes
- Striped volumes
- RAID-5 volumes

For all supported Microsoft Windows, operating systems that restor a volume to dynamic disk require restoring the volume to a basic disk. After restore the volume to a basic disk, convert the disk to dynamic disk. You cannot restore a volume directly to a dynamic disk.

Note: If you use a Microsoft Window 2008 32-bit or 64-bit operating system, you cannot complete a volume-level restore for a simple dynamic disk. Instant Restore and a file-level restore work for these operating systems.

Backup considerations

During the snapshot of any dynamic disk other than a simple volume, there is the potential for increased memory utilization on the protected server. This increase might result in the snapshot not completing. This exposure exists when there are many data changes while the snapshot is running.

Backup success is based on the amount of memory available and the I/O load for Copy-On-Write (COW) when the snapshot runs on the protected server. If the I/O activity causes available memory limits to be exceeded, a FastBack Client system is limited to no more than 2 GB virtual address space (32–bit support limitation), the process terminates. The termination of a snapshot does not affect production I/O, but it does affect the Recovery Point Objective (RPO).

This exposure does not exist on volumes that are mapped to a single LUN (for example, basic disks or simple dynamic disks).

To alleviate the risk of these types of snapshots that are being terminated, complete the following tasks:

1. Reduce the quantity of Copy-On-Write data during a snapshot. For example, schedule snapshots during time periods with less I/O activity.
2. Reduce the time that is required to complete a snapshot. For example, you can schedule more frequent snapshots. Balance the scheduling of frequent snapshots with the likelihood of encountering higher I/O activity when the snapshot runs.

   You can also reduce the time that is required to complete a snapshot by using a SAN backup, instead of a LAN backup.
3. Verify that the FastBack Server hardware is configured for optimal snapshot performance. For example, ensure that you use the highest performing storage device for the FastBack Server repository.

In addition, Continuous Data Protection is not supported for dynamic disks.

Restore considerations

Volume restore and instant restore are only possible to basic disks and to simple volumes that are used in supported operating system environments. Restoring a volume to dynamic disk requires restoring the volume to a basic disk. After you restore the volume to a basic disk, convert the disk to dynamic disk. You cannot restore a volume directly to a dynamic disk.

Regular bare machine recovery disks can be converted to dynamic disks by completing the following steps:

1. Log on as Administrator, or as a member of the Administrators group.
2. Open the Performance and Maintenance Control Panel, click **Administrative Tools**, and then double-click **Computer Management**.
3. In the navigation pane, click **Disk Management**.
4. In the pane that displays the disks, right-click the basic disk that you want to convert; then, click **Convert to Dynamic Disk**.

   Note: The disk title is on the left side of the Details pane. Right-click the gray area that contains the disk title.
5. If it is not selected, select the check box next to the disk that you want to convert. Click **OK**.
6. If you want to view the list of volumes in the disk, click **Details**.
7. Click **Convert**.
8. When prompted, click **Yes**.
9. Click **OK**.

If you remove one of the two disks in the software mirror, the remaining signature changes for the disk. If this result occurs, complete the following steps:

1. Delete the new chain.

2. In the `history.txt` file, replace old signatures with the new signature for all snapshots from the old chain. To get this number, right-click to select the remaining drive. Select **Properties**. The signature is displayed in the window.

Support for cluster environments

Microsoft Cluster Server (MSCS) does not natively support dynamic disks.

In the Veritas Cluster Server (VCS) environment, simple and spanned volumes are the only types of supported dynamic disks. The backup and restore considerations for dynamic disks apply in a VCS environment.

Veritas Storage Foundation for Windows provides a Cluster Option for MSCS. This option adds a cluster resource for dynamic disks to be used in an MSCS cluster. This configuration is not supported.

Dynamic disks that are created with Veritas Storage Foundation for Windows that are not in a cluster environment are not supported.

Software requirements and prerequisites

To install Tivoli Storage Manager FastBack, various applications, utilities, and components must first be installed or available.

Administrative Command Line (Linux only)

To use the Administrative Command Line from a system that runs a supported Linux operating system, complete the following steps:

1. On the system where you installed or plan to install the Administrative Command Line, install Cygwin 1.5.25 or later. When you install Cygwin, include the OpenSSH package. To manually install Cygwin, complete the following steps:

   a. Log on to the Windows server with an account that has administrator privileges.

   b. Go to the following website and install Cygwin 1.5.25 or later: http://www.cygwin.com

   c. When completing the installation wizard for Cygwin, there is a **Select Package** page. On this page, clear the **Hide obsolete and administrative packages** check box.

   d. During the installation process for Cygwin, select the following Cygwin packages:

Table 16. Cygwin packages

Category	Package
Net	All default packages. In addition, select the following packages: • **openssh** (contains **ssh.exe**) • **openssl** (contains **ssl.exe**) • **rsync** • **tcp_wrappers**

e. After finishing the Cygwin installation wizard, add the `Cygwin\bin` directory to the Microsoft Windows %PATH% environment variable. The directory must be the first one in the %PATH% environment variable.

> **Remember:** Restart the system so the variable update can take effect.

2. On the system where you installed or plan to install the Administrative Command Line, test the Cygwin installation.

   > **Remember:** Before using Cygwin, review the Cygwin documentation for any issues that might affect your environment.
   > To test the Cygwin installation, from the Microsoft Windows Start menu, select **Programs** > **Cygnus Solutions** > **Cygwin Bash Shell**. A command prompt window is displayed. This window is a bash shell.

3. On the system where you installed or plan to install the Administrative Command Line with Cygwin, install the SSH daemon service. To install the SSH daemon service, complete the following steps:

   a. Enter the following commands to give read access to the `/etc/passwd` and `/etc/group` files:
   ```
   chmod +r /etc/passwd
   chmod +r /etc/group
   ```

   b. Enter the following command to give read access to the `/var` directory:
   ```
   chmod 755 /var
   ```

   c. From the Cygwin command prompt window, run the following command to create the SSH daemon service:
   ```
   ssh-host-config
   ```

   d. When a query about whether privilege separation must be used is posted in the command prompt window, enter *no*.

   e. When a query about whether a new local account named *sshd* must be created is posted in the command prompt window, enter *yes*.

   f. When a query about whether *sshd* must be installed as a service is posted in the command prompt window, enter *yes*.

   g. When you are asked to enter the value of **CYGWIN** for the daemon, enter the following text: *ntsec tty*

   h. When you are asked if you want to use a different name, enter *no*.

   i. When you are asked if you want to create a new privileged user account named *cyg_server*, enter *yes*.

   j. When you are asked to enter a password, enter a password. You are asked to reenter the password to confirm the entry. The host configuration is complete. A status message is displayed.

   k. At the prompt, enter the following command:
   ```
   set CYGWIN 'ntsec tty'
   ```

   Also, add CYGWIN as a Microsoft Windows environment variable with the value `ntsec tty`.

4. Configure the authentication key files by logging on to the Linux system where FastBack Client is installed and completing these tasks:

   a. Issue this command and press **Enter** at all prompt questions:
   ```
   ssh-keygen -t dsa
   ```

   b. Issue these commands:

```
cd .ssh
scp id_dsa.pub Administrator@windows_machine:/home/Administrator
```

c. Issue these commands from the Cygwin shell on the Windows server:

```
mkdir .ssh
chmod 700 .ssh
cd .ssh
touch authorized_keys
cat ../id_dsa.pub >> authorized_keys
rm ../id_dsa.pub
```

d. Configure the SSH server to use the authentication files by editing the SSH service configuration file c:\cygwin\etc\sshd_config. Open this file and unmark these entries:

```
Protocol 2
HostKey /etc/ssh_host_dsa_key
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile
```

Update the AuthorizedKeysFile value to specify /home/Administrator/.ssh/authorized_keys.

e. Issue these commands from the Cygwin shell on the Windows server to restart the sshd service:

```
net stop sshd
net start sshd
```

f. Verify that the Linux system can communicate with the Windows server system by issuing this command (from the Linux system):

```
ssh Administrator@windows_machine
```

SSH attempts to update the known_hosts file for each host name convention specified. For example, although all of these commands identify the same Windows Server, SSH attempts to add an entry to the known_hosts file for each host name:

```
ssh Administrator@windows_machine
ssh Administrator@windows_machine.xyz.com
```

To prevent possible timeout errors from authentication failures, implement one (or both) of these recommendations:

• Consistently use the same host name convention when accessing the Windows Server.

• Update the known_hosts file with all host name conventions associated with the Windows Server.

Important: You must create authentication key files for each new client system. Therefore, complete Steps 4a through 4f for each client system.

5. Allow any host to connect with SSH to the server by editing the following file: C:\cygwin\etc\hosts.allow

The following line needs to immediately precede the ALL : PARANOID : deny line:

```
sshd: ALL
```

6. After the FastBack Server, FastBack Client, and Administrative Command Line components are installed, from the Linux system where you installed FastBack Client, connect to the FastBack Server system with Cygwin and the SSH daemon service.

7. Log on to the Administrative Command Line (without a password).

8. In the command prompt window, enter the following command:

```
FastBackShell.exe -c command type tag parameter
```

In addition to the Cygwin and SSH daemon service, the GNU C libraries, Version 2.3.3-98.38 or later are required.

FastBack Client (Windows 2003 only)

Before you install the FastBack Client on a supported Windows 2003 operating system, ensure that the following Windows components are installed:

- The Distributed Transaction Coordinator (MSDTC) service
- Component Services (COM+)

For more information about installing these components, see the documentation for your operating system.

If you do not install these components, or, if these components are not working correctly, the FastBack Client installation fails. To work around this problem, complete the following steps:

1. Reinstall the component that is not installed or not working correctly.
2. Uninstall FastBack Client.
3. Reinstall FastBack Client.
4. Retry a FastBack Client snapshot for the machine.

FastBack Client (Linux only)

FastBack Client can back up and restore volumes on the following types of file systems.

Table 17. File systems supported for volume backup and restore by FastBack Client

File system	Support type
EXT2	Content aware
EXT3	Content aware
ReiserFS	Non-content aware

Note: In this context, *content aware* support means that you can restore the files on a partition to the partition from where they originated.

Important: Any hard disk that is backed up with Tivoli Storage Manager FastBack needs to have a disk signature, a disk identifier usually provided by the operating system. FastBack Client requires that every disk to be backed up has a unique and nonzero signature.

Because hard disks for Linux operating systems frequently do not have such signature, such disk is not counted by FastBack Client and is not displayed in the FastBack Manager.

The FastBack Disk Signature utility can be used to check and to change (if required) the disk signature of hard disk. The FastBack Disk Signature is the command line tool receiving only one argument, the name of the disk to check the signature for.

To run the FastBack Disk Signature utility, complete the following steps:

1. From a command-line window, change directories to the FastBack Client installation directory. By default, the path to this directory follows: /opt/IBM/Tivoli/TSM/FastBack/client

2. Use the following code examples to run the FastBack Disk Signature utility. The utility is called by the FastBackDiskSignature command. When the utility is called without parameters, the following output is printed:

```
#./FastBackDiskSignature
Usage: ./dsig /dev/<disk_name>
```

When the provided disk name is invalid in the system, an error message is provided:

```
#./FastBackDiskSignature /dev/abc
Invalid disk name: /dev/abc
```

If the disk name is the correct the current disk signature value is displayed and the user is prompted to change it:

```
# ./FastBackDiskSignature /dev/sda
Disk /dev/sda has signature 00000000.
Enter new signature (Enter to put 4AE71A19, Ctrl-C to cancel):

#./FastBackDiskSignature /dev/sda
Disk /dev/sda has signature 30307800.
Enter new signature (Enter to put 4AE71A22, Ctrl-C to cancel):
```

You can type a new signature or press enter to accept the suggested signature value.

To exit the utility, enter **CTRL-C**.

FastBack Manager and FastBack Server

(Windows 2008 only) Before installing FastBack Manager on a computer with the Microsoft Window 2008 operating system, Internet Protocol version 6 (IPv6) must be disabled. If IPv6 is not disabled, a message indicates that the system cannot connect to FastBack Manager. For information about how to disable IPv6, see the Microsoft Knowledge Base article 929852 online at http://support.microsoft.com/kb/929852.

When you install the FastBack Server, the FastBack Server needs to be added as a member of a domain, not a workgroup. In addition, when planning for communication between the FastBack Server and FastBack Client, if the server is set up as a multihomed host, the FastBack Server listens to only one connection. The FastBack Server listens to the first connection that is listed. The clients that try to connect to the second IP address return a message that indicates that the connection failed.

One FastBack Manager system can control multiple branches by running multiple instances of FastBack Manager GUI. If there is more than one FastBack Server in a branch, only one FastBack Server can be controlled by an external FastBack Manager because a port can be forwarded to only one destination.
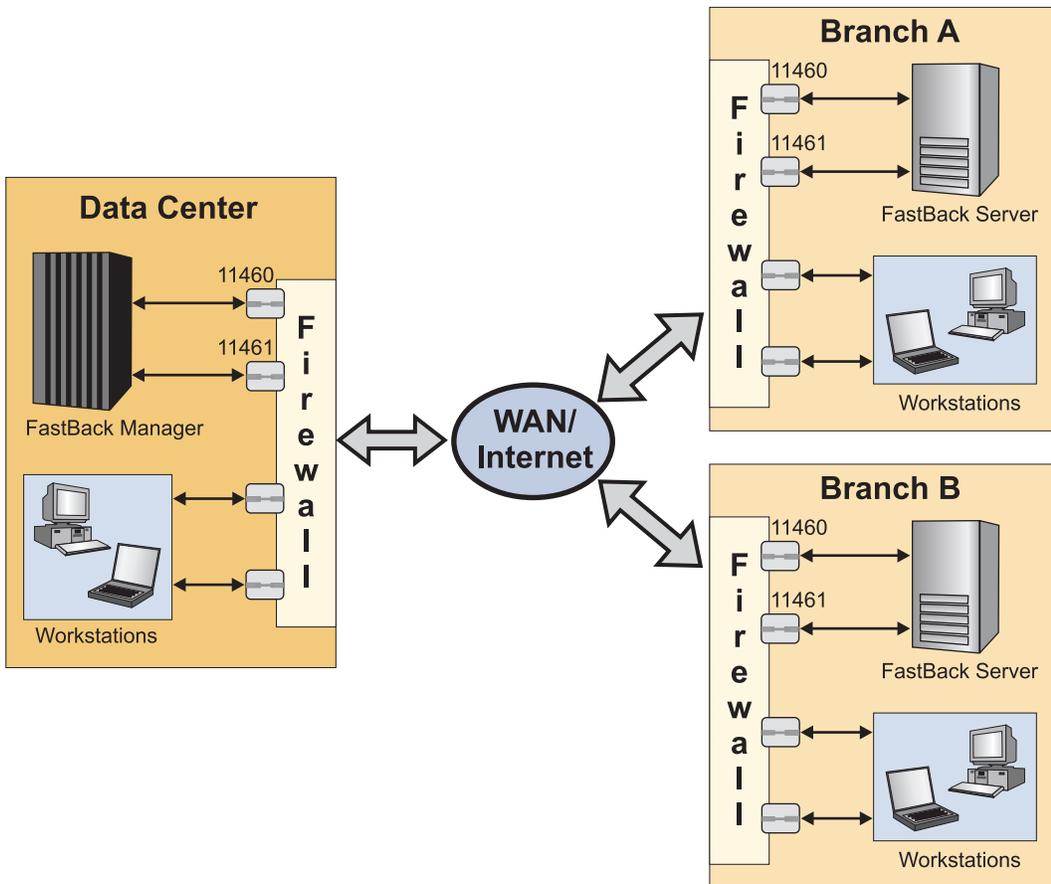
Figure 4. Controlling multiple branches from the Data Center

The following ports must be opened in a firewall, and the ports must be forwarded to FastBack Manager and FastBack Server:

TCP   11460

UDP   11461

The following ports must be opened in a firewall, and the ports must be forwarded to the FastBack Server and FastBack Client:

TCP   11406

TCP   1320

The following ports must be opened in a firewall, and the ports must be forwarded to the FastBack Server and FastBack Disaster Recovery Hub server:

TCP (Active FTP)
    20, 21, 1023

TCP (Passive FTP)
    21, 1023

All the sensitive information such as user names, passwords, and domain names, is transferred with Triple DES encryption. FastBack Manager can connect to FastBack Server over T Carrier lines (T1, T2, T3). Usability is subject to quality of service of the connection.

FastBack Mount

FastBack Mount uses the Microsoft Common Internet File System (CIFS) protocol to connect to the repository. Port 445 must be open for FastBack Mount to work correctly.

Users must be logged in locally to run FastBack Mount operations. FastBack Mount cannot be used when it is accessed through a remote desktop connection.

Anti-virus and anti-spyware software

If you use anti-virus and anti-spyware software, consider that anti-virus and anti-spyware applications might interfere with Tivoli Storage Manager FastBack operations. The anti-virus and anti-spyware applications can damage the Tivoli Storage Manager FastBack database and log files, resulting in data loss.

In addition, when anti-virus and anti-spyware applications run simultaneously with FastBack Mount, there is high processor usage, resulting in snapshots running slowly or being stopped. In rare cases, running FastBack Mount with anti-virus and anti-spyware applications can also cause a Windows system crash. If a system crash occurs, reboot the system. The system will start normally.

When using anti-virus and anti-spyware software, exclude the following folders from file-level scanning:

- Tivoli Storage Manager FastBack log and configuration files folder and all its subfolders, including the default, `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\`
- Tivoli Storage Manager FastBack program files folder and all its subfolders, default `C:\Program Files\Tivoli\TSM\FastBack\`
- Tivoli Storage Manager FastBack repository disks and folders.
- Mount points to any repository disks.

If you move any Tivoli Storage Manager FastBack folders to a new location, for example, changing the staging area path, or adding and moving repositories, remember to exclude those new folders or disks as well.

For information about how to add disks or folders to the exclusion list, see your anti-virus and anti-spyware software documentation. Make sure that your anti-virus and anti-spyware software is up to date.

Follow these guidelines when using anti-virus and anti-spyware software in conjunction with Tivoli Storage Manager FastBack :

- Do not schedule scans and to run simultaneously with snapshots.
- Before running manual or scheduled scans on the repository disks, you must stop the FastBack Server service. Do not mount or restore snapshots from this repository with FastBack Mount during scans.
- Volume or disk restore can fail or run slowly if anti-virus and anti-spyware software is configured to real-time or manual scan on one of the destination volumes or disks. Cancel scans of the volume or disk before starting the restore process.
- Some anti-spyware software can falsely recognize some Tivoli Storage Manager FastBack components as spyware, because of high traffic volume. Tivoli Storage Manager FastBack does not contain any spyware, adware, or viruses.

- If you want to restore a large number of files from a virtual volume, created by FastBack Mount, before restoring, this volume must be excluded from anti-spyware, adware, and virus protection scanning.

FastBack Reporting (Windows only)

On the system where you are going to install and use FastBack Reporting, your system must meet the following software prerequisites:

- IBM Tivoli Common Reporting, Version 1.2 Fix Pack 1. You can download Tivoli Common Reporting, Version 1.2 Fix Pack 1 from the Passport Advantage online website at http://www.ibm.com/software/howtobuy/passportadvantage/ pao_customers.htm. The installation instructions are online at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/ com.ibm.tivoli.tcr.doc/ttcr_install.html.

  For more information about Tivoli Common Reporting, see http:// www.ibm.com/developerworks/spaces/tcr. For the Tivoli Common Reporting Information Center, see http://publib.boulder.ibm.com/infocenter/tivihelp/ v3r1/topic/com.ibm.tivoli.tcr.doc/tcr_welcome.html.

- FastBack Server, Version 6.1.0. For more information, see FB_InstallUse/ FB_InstallUse/t_fast_install_fb_server.dita.

- Web browser supported by Tivoli Common Reporting, Version 1.2 Fix Pack 1. For more information, see http://publib.boulder.ibm.com/infocenter/tivihelp/ v3r1/topic/com.ibm.tivoli.tcr.doc/ctcr_supported.html.

Microsoft Cluster Server (MSCS) and Veritas Cluster Server (VCS) (Windows only)

During the installation of the FastBack Client software on the cluster nodes, you are required to restart the system. Perform the client installation on one system at a time to ensure a smooth failover and failback operation.

When you install the FastBack Client, by default, the SAN Module option is disabled. Use the FastBack Client Configurator to enable the SAN Module option. This setting is required for a cluster environment because when nodes switch, incremental delta block snapshots need to occur.

In a cluster environment, every local disk at each node is to have a different disk signature. For example, if *disk1* on *node1* has the same signature as *disk1* on *node2*, an error might occur.

For information about the FastBack Client Configurator, see "Connecting client to server" on page 87.

When using Tivoli Storage Manager FastBack in a cluster environment, the following statements of support apply:

- FastBack Client and FastBack Mount are supported in a cluster environment. FastBack Server is not supported in a cluster environment.

- You can restore a Microsoft Exchange Server 2007 volume backup, either snapshot or CDP, taken from an LCR or CCR replica or production volume.

- You can restore a Microsoft Exchange Server 2010 volume backup, either active database copy or passive database copy, taken from a Database Availability Group (DAG) or production volume.

- In a cluster environment, when running bare machine recovery, direct bare machine recovery to a cluster disk, including a quorum disk, is not supported. However, you can remove the disk from the cluster before starting a bare machine recovery. After bare machine recovery is complete, you can return the disk to the cluster.
- A volume restore to a volume on a cluster disk, including a quorum disk, is not supported. In this scenario, FastBack Mount is to be used to retrieve data.
- Microsoft Exchange 2003 clusters that are running on Microsoft Windows 2003 are supported.
- Microsoft SQL 2005 clusters that are running on Microsoft Windows 2008 (64 bit) are supported.

For information about managing the Microsoft Cluster Server (MSCS) and Veritas Cluster Server (VCS) environments during restoration of a cluster volume using instant restore, see "Instant restore for Microsoft Cluster Server (Windows only)" on page 131 and "Instant restore for Veritas Cluster Server (Windows only)" on page 132.

Chapter 3. Installing and upgrading

Before beginning the installation or upgrade process, verify that your system meets all operating system, hardware, and software requirements.

For the system requirements, see the Chapter 2, "Planning," on page 9 section.

For Tivoli Storage Manager FastBack, Version 6.1.7, you can complete a new installation or upgrade from Tivoli Storage Manager FastBack, Version 5.5.x or 6.1.x to Tivoli Storage Manager FastBack, Version 6.1.7. The following versions are compatible:

- FastBack Server 6.1.7 and FastBack Client 6.1.7
- FastBack Server 6.1.7 and FastBack Client 5.5.4 and later
- FastBack Server 6.1.7 and FastBack Client 5.5.4 and FastBack Client 6.1.x

When you upgrade from Tivoli Storage Manager FastBack, Version 5.5.x or 6.1.x to Tivoli Storage Manager FastBack, Version 6.1.7, the data is migrated. For example, any user IDs, user groups, schedules, and policies that you created are available when using Tivoli Storage Manager FastBack, Version 6.1.7.

By default, when you install FastBack Server, FastBack Manager is installed. Using the `Advanced` installation option, you can also install FastBack Manager on a computer without installing FastBack Server. In this scenario, when you upgrade the Tivoli Storage Manager FastBack software, you do not have to upgrade FastBack Server before you upgrade FastBack Manager; the upgrade order for these systems does not matter. When deployed in a production environment, the FastBack Server and FastBack Manager computers must use the same version of the software.

Installing the server and client components

For purposes of performance and disaster recovery, it is always best that the FastBack Server and FastBack Client have dedicated and separate hardware resources available. Installing the server and client on separate systems is advised so that there is sufficient disk I/O and processor available to carry out the scheduled workloads, and available repository disk access for recovery in the event that the FastBack Client system experiences a disaster.

In situations where FastBack Server and FastBack Client components are installed and running on a single operating system or physical machine, it is important that sufficient resources be made available (for example, memory, processor, disk I/O) to each component on this shared system. On systems or servers with insufficient resources, it is necessary to separate the server and client components to separate dedicated servers to improve throughput and response times.

If you install the server and client on the same system, the following list of limitations is applicable:

- The client installed on the same system as the server must be configured as *SAN enabled*. This configuration is required regardless of SAN disks.
- After you install the software, you need to create a repository to back up data. For more information about repositories, see "Repositories" on page 93.

- When the server and client are installed on the same system, disk-based repositories cannot be used. Volume and folder repositories can be used.

Note:

- When FastBack Server is installed on the same machine as FastBack Client, data loss may occur. FastBack Server may be installed unintentionally when a user selects the default installation option when using the 64-bit FastBack installer to install the FastBack Client.
- If you do install FastBack Server and the FastBack Client on the same machine, you can prevent data loss by running the disk open utility. For more information on how to use the disk open utility, see Allowing read/write access to a disk with disk open utility.

Upgrading the server and client components

When upgrading the FastBack Server and FastBack Client, upgrade the FastBack Server first. The FastBack Server version must be greater than or equal to the FastBack Client version. In addition, if you install a FastBack DR Hub Server, the FastBack DR Hub Server version must be greater than or equal to the FastBack Server version.

When upgrading the FastBack DR Hub Server from Version 6.1.x to Version 6.1.7, the IBM Global Security Kit (GSKit) 8 registry key is not automatically updated. You must manually update the registry key before upgrading the FastBack DR Hub Server to Version 6.1.7. Update the `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK8\CurrentVersion\CryptLibPath` value to specify `C:\Program Files\IBM\GSK8\lib`.

FastBack Reporting (Windows only)

The FastBack Reporting installation process is separate from the Tivoli Storage Manager FastBack installation process. You cannot choose to install FastBack Reporting from the Tivoli Storage Manager FastBack installation wizard.

Prerequisite tasks

Before you begin

All applications that relate to Tivoli Storage Manager FastBack are to be closed before attempting to install, upgrade, maintain, or uninstall the product.

(Windows only) When you run the installation or upgrade process, use a Windows logon ID with Administrator authority.

(Linux only) Run the installation process as the root user. The root user profile must be sourced. If you use the **su** command to switch to root, use the **su -** command to source the root profile.

(Linux only) Ensure that the file `/etc/hosts` contains the following text:

`127.0.0.1 localhost`

Before starting the installation or upgrade process for FastBack Server, disconnect the computer from the storage area network (SAN) by disconnecting the fiber optic cable.

Reconnect the system only after the FastBack Server is installed or upgraded, and the system is restarted.

The installation logs are stored in %ALLUSERSPROFILE%\FastBackInstallation.log.

Installing Tivoli Storage Manager FastBack using the installation wizard

About this task

During the Tivoli Storage Manager FastBack installation process, you can choose to install services and interfaces by selecting the appropriate options:

Backup Client
Install on production and application servers that need backup protection. When you select this option, you install the following components:
- FastBack Client
- FastBack Mount

    This component is installed by default on Windows and as a separate component of Linux.
- Administrative Command Line

Backup Server (32 bit only) (Windows only)
Install the FastBack Server software on the system you designate to be the backup server. When you select this option, you install the following components:
- FastBack Server
- FastBack Mount
- Administrative Command Line
- FastBack Disaster Recovery
- Documents
- FastBack Manager

Disaster Recovery Server (32 bit only) (Windows only)
Install on the server that you use to back up a FastBack Server. When you select this option, you install the following components:
- FastBack Manager
- FastBack DR Hub Server
- Central Control Station
- Administrative Command Line
- FastBack Mount
- Documents

Advanced
Installs services and interfaces that you select. The space requirements for the options you select are displayed under the list of options.

The descriptions that are provided for the modules are brief. For more information, see the wizard for the installation process.

When you install the Tivoli Storage Manager FastBack on 64-bit environments, you are given the option of a complete installation or a custom installation. You can install the full version by selecting complete or you can choose what services and

interfaces to install by selecting the custom option.

Installing FastBack Server (Windows only)

Administrator privileges are required to install Tivoli Storage Manager FastBack. The FastBack Server must be installed on the system that is designated as the backup server.

Before you begin

You must disconnect the FastBack Server system from the SAN until the FastBack Server installation is complete and the system is restarted.

About this task

To install the FastBack Server on a Microsoft Windows 2003, Windows 2008, or Windows XP x86 system, complete the following steps:

Procedure

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the X86 folder.
3. Start the installation program.
4. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.
5. Read the terms of the license agreement. To accept the license agreement, click **Yes**. You must accept the terms of the license agreement to continue the installation.
6. A page is displayed prompting you to specify the destination folder where the FastBack Server is to be installed. Accept the default location, or click **Browse** to go to the location. Click **Next**.
7. A page is displayed prompting you to select the **Installation Type**. Select **Backup Server**. Click **Next**.
8. Click **Next**.
9. (Optional) A message about the virtual volume driver not installing for FastBack Mount might be displayed. Click **OK** to accept the message.
10. The software is installed. To complete the installation of the FastBack Server, restart the computer. Click **Finish**.
11. (Optional) After the restart, reconnect the FastBack Server to the SAN. Use LUN masking to enable the FastBack Server to see the SAN disks that are backed up.

Results

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:
- Modify - Use this option to change the location of the installation.
- Remove - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing FastBack Server on Windows Server 2008 R2
Before you begin

- If the system is connected to LUNs in a SAN environment, and SAN backups are planned, disconnect the Fibre Channel cable. When iSCSI is used, disconnect the network cable. Reconnect the cable after the installation and system restart complete. See "Configuring SAN environment" on page 89 for more details.
- If antivirus software is installed on the Windows Server 2008 R2 system, you must configure the antivirus software to exclude the following paths before you install the FastBack Server:
  - `C:\ProgramData\Tivoli\TSM\FastBack\`
  - `C:\Users\All Users\Tivoli\TSM\FastBack\`
  - All repository locations.
- The FastBack Mount component must be selected and installed in order for FastBack Server to function.

About this task

To install the FastBack Server on a Windows Server 2008 R2 x64 system, complete the following steps:

Procedure

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the X64 folder.
3. Start the installation program.
4. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.
5. Read the terms of the license agreement. To accept the license agreement, click **Yes**. You must accept the terms of the license agreement to continue the installation.
6. Select the type of installation:

Table 18. Tivoli Storage Manager FastBack components

Complete	Custom

Installs all of the following components:
 	
`FastBack Mount`
`FastBack Client`
`Administrative Command Line`
`Documents`
`Central Control Station`
`FastBack DR Hub Server`
`FastBack Server`
` FastBack Data Deduplication Service`
`FastBack Manager`
	All components and subcomponents are already selected. Select the items that you do not want to install.

When `Custom` is selected, you are prompted to specify the destination folder where the FastBack Server is to be installed. Accept the default location `C:\Program Files(x86)\Tivoli\TSM\FastBack` or click **Change** to go to a different location. Click **Next**.
7. You are prompted to begin installation. Click **Next** to proceed.
8. When installation completes successfully, you can start Tivoli Storage Manager FastBack by selecting the `Launch IBM Tivoli Storage Manager FastBack for`

x64 option in the Installation Wizard Completed panel and clicking **Finish**. You are prompted to restart the system. A system restart is required for the FastBack Server to start properly. Click **Yes**.

Tip: When you install the FastBack Server as a modification or repair, you are not prompted to restart the system. However, a system restart is still required for the FastBack Server to start properly.

Results

After successfully installing the FastBack Server on a Windows Server 2008 R2 x64 system, see Chapter 5, "Starting and configuring," on page 77 for more information about using Tivoli Storage Manager FastBack.

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:
- `Modify` - Use this option to change the location of the installation.
- `Remove` - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing FastBack Client
Before you begin

(Windows only) When you run the installation or upgrade process, use a Windows logon ID with Administrator authority.

(Linux only) Run the installation process as the root user. The root user profile must be sourced. If you use the **su** command to switch to root, use the **su -** command to source the root profile.

Tip: If the Red Hat Enterprise Linux 5.4 Server installer terminates abruptly (for example, CTRL+C was issued), remove all log files in the `usr/ibm/common/acsi/logs/` directory before you start another installation attempt. The installer might remain blocked until these logs are removed.

If you are installing the FastBack Client on a 64-bit operating system, you might notice slight differences in the installation wizard pages.

About this task

To install the FastBack Client, complete the following steps:

Procedure
1. Either download the installation file or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the folder that corresponds with your system. For example, there are folders that are labeled IA64, X64, and X86. In addition, there are folders for the various language packs.
3. (SELinux only) Temporarily disable SELinux before you run the installation program. To temporarily disable SELinux, enter the following command:
   `/usr/sbin/setenforce 0`
4. Start the installation program.

5. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.
6. Read the terms of the license agreement. You must accept the terms of the license agreement to continue the installation.
7. Depending on your system, use one of the following procedures to complete the installation process:
   - For Linux systems, complete the following steps:
     a. The installation wizard displays information about the Deployment Engine initialization. Click **Next**.

        Note: If the Deployment Engine fails to initialize, remove all .lock* files in the `/usr/ibm/common/acsi/logs/` directory, and restart the wizard.
     b. If you do not want to use the default installation directory, choose another installation directory. Click **Next**.
     c. Select **Backup Client**. Click **Next**.
     d. The components that are selected for installation are displayed. Click **Next**.
     e. Type the host name or IP address for the FastBack Server. Click **Next**.
     f. A pre-installation summary window is displayed. Review the summary. If you want to change any installation options, click **Previous**. If you want to install the components, click **Install**.
     g. The software is installed. To complete the installation of the FastBack Client, restart the computer.
   - For Windows 32-bit systems, complete the following steps:
     a. A page is displayed prompting you to specify the target directory where the software is to be installed. Accept the default location that is displayed in the `Directory Name` field, or type over it to specify the location, or click **Browse** to navigate to the location. Click **Next**.
     b. A page is displayed prompting you to select the Installation Type. Select **Backup Client**. Click **Next**.
     c. (Optional) A message about the virtual volume driver not installing for FastBack Mount might be displayed. Click **OK** to accept the message. You must accept this message to complete the installation.
     d. Type either the DNS name of the FastBack Server system (must be unique in the network), or, enter the IP address if a static IP address is used. The name cannot contain a space.
     e. Click **Next**.
     f. The software is installed. To complete the installation of the FastBack Client, restart the computer. If you do not restart the computer, the client service is not active and the client status is listed as stopped.
   - For Windows 64-bit systems, complete the following steps:
     a. (Optional) A message about the virtual volume driver not installing for FastBack Mount might be displayed. Click **OK** to accept the message. You must accept this message to complete the installation.
     b. Information about the installation is displayed. Click **Next**.
     c. The software is installed. To complete the installation of the FastBack Client, restart the computer. If you do not restart the computer, the client service is not active and the client status is listed as *stopped*.
     d. After the system restarts, from the Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Client Configurator**.

e. If prompted, type the host name or IP address for the FastBack Server.

f. Click **OK**.

What to do next

If the client has only DAS disks, no additional steps are required. When you install the FastBack Client, by default, the `SAN Module` option is disabled. Use the FastBack Client Configurator to enable the `SAN Module` option when you use CLUSTER or LANFREE.

If the client has SAN disks, configure the client according to the following steps:

1. From the Start menu, choose **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Client Configurator**.
2. Verify the DNS host name or IP address for the FastBack Server system.
3. If you have a cluster environment, enable the `SAN Module` option.
4. Click **OK**.

You can also use the FastBack Client Configurator to connect a FastBack Client to a FastBack Server. To use the FastBack Client Configurator to connect a FastBack Client to a FastBack Server, complete the following steps:

1. On the computer where you installed FastBack Client, from the Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Client Configurator**.
2. Type the host name or IP address for the FastBack Server.
3. Click **OK**.

After you connect a client to a server through the Client Configurator, in the FastBack Manager, you might not see the client in the client list. A client version mismatch is the cause of the problem. To resolve this problem, verify that both the client and the server are using the same version of Tivoli Storage Manager FastBack. After you install the correct version, restart both the client and server by using the Windows Services. To go to to the Services window, click **Control Panel** > **Administrative Tools** > **Services**.

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:

- `Modify` - Use this option to change the location of the installation.
- `Remove` - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing FastBack DR Hub Server (Windows only)

Installing the FastBack DR Hub Server is required if you want to back up a FastBack Server repository. In addition, install the FastBack DR Hub Server if you want to have a central site in the Tivoli Storage Manager FastBack environment.

Before you begin

The communication between the FastBack Server in a remote location and the FastBack DR Hub Server in a central site or disaster recovery location is based on extensions to the standard FTP protocol. As such, the installation of the FastBack DR Hub Server requires that you install a standard FTP server on the system that hosts the FastBack DR Hub Server.

The installation process for the FastBack DR Hub Server requires that you complete the following tasks:

1. Install an FTP server on the system to be used as the FastBack DR Hub Server. For installation instructions, see the product documentation for the FTP server.

   You can use compression and encryption with the FastBack Disaster Recovery if the FTP server supports these features. Select an FTP server that supports compression and encryption. If you enable encryption on the FastBack Disaster Recovery server, SSL must be enabled on the FTP server.

2. Install the FastBack DR Hub Server. To install the FastBack DR Hub Server, complete the following steps:

   a. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.

   b. Go to the Tivoli Storage Manager FastBack X86 folder.

   c. Start the installation program.

   d. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.

   e. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. You must accept the terms of the license agreement to continue the installation.

   f. A page is displayed prompting you to specify the target directory where the software is to be installed. Accept the default location that displayed in the **Directory Name** field, or type over it to specify the location, or click **Browse** to go to the location. Click **Next**.

   g. A page is displayed prompting you to select the **Installation Type**. Select **Disaster Recovery Server**. When you install the Disaster Recovery Server, you install the FastBack DR Hub Server, Central Control Station, FastBack Manager, and FastBack Mount.

   h. Click **Next**.

   i. If you are in a DHCP environment, enter either the IP address or the name of the FastBack Server (if your DHCP environment supports name registration). If your FastBack Server has a static IP address, enter either the IP address or the name of the FastBack Server. The FastBack Server name cannot contain a space.

   j. Click **Next**.

   k. The software is installed. To complete the installation, restart the system.

3. Configure the FastBack DR Hub Server. For configuration instructions, see "Setting up FTP for the disaster recovery destination (Windows only)" on page 195 and "Configuring FastBack Server Disaster Recovery with an FTP server" on page 202.

4. Configure the Central Control Station. For configuration instructions, see "Using Central Control Station (Windows only)" on page 211.

Results

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:

- `Modify` - Use this option to change the location of the installation.
- `Remove` - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing with Advanced options

When you select the `Advanced` type of installation, you can select the services and interfaces to install. The space requirements for the selected options are displayed under the list of options in the installation wizard.

When installing FastBack Mount, you want to install FastBack Mount on the systems where you want to mount snapshots and perform an instant volume restore.

(Windows only) For Central Control Station, install at the central backup office or Data Center. You can use Central Control Station to browse for snapshots and events stored in the FastBack DR Hub Server database.

Installing FastBack Manager
Before you begin

(Windows only) When you run the installation or upgrade process, use a Windows logon ID with Administrator authority.

(Linux only) Run the installation process as the root user. The root user profile must be sourced. If you use the **su** command to switch to root, use the **su -** command to source the root profile.

About this task

To install FastBack Manager, complete the following steps:

Procedure

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. Go to the Tivoli Storage Manager FastBack X86 folder.
3. (SELinux only) Temporarily disable SELinux before you run the installation program. To temporarily disable SELinux, enter the following command: `/usr/sbin/setenforce 0`
4. Start the installation program.
5. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.
6. Read the terms of the license agreement. You must accept the terms of the license agreement to continue the installation.
7. Depending on your system, use one of the following procedures to complete the installation process:
   - For Linux systems, complete the following steps:
     a. The installation wizard displays information about the Deployment Engine initialization. Click **Next**.
     b. If you do not want to use the default installation directory, choose another installation directory. Click **Next**.
     c. Select **FastBack Manager**. Click **Next**.
     d. The components that are selected for installation are displayed. Click **Next**.
     e. Type the host name or IP address for the FastBack Server. Click **Next**.

f. A pre-installation summary window is displayed. Review the summary. If you want to change any installation options, click **Previous**. If you want to install the components, click **Install**.

g. The software is installed. To complete the installation of the FastBack Client, restart the computer.

- For Windows systems, complete the following steps:

  a. A page is displayed prompting you to specify the target directory where the software is to be installed. Accept the default location that is displayed in the **Directory Name** field, or type over it to specify the location, or click **Browse** to go to the location. Click **Next**.

  b. A page is displayed prompting you to select the **Installation Type**. Select **Advanced**.

  c. Click **Next**.

  d. Select **FastBack Manager**. Following the list of features that you can select for installation, the space requirements are displayed.

  e. If you are in a DHCP environment, enter either the IP address or the name of the FastBack Server (if your DHCP environment supports name registration). If your FastBack Server has a static IP address, enter either the IP address or the name of the FastBack Server. The FastBack Server name cannot contain a space.

  f. Click **Next**.

  g. The software is installed. To complete the installation, restart the system.

Results

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:

- `Modify` - Use this option to change the location of the installation.
- `Remove` - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing the Administrative Command Line (Windows only)
Before you begin

You cannot install the Administrative Command Line on a system that is running a Linux operating system. However, you can use the Administrative Command Line from a system that is running a supported Linux operating system. For more information, see "Software requirements and prerequisites" on page 33.

When you run the installation or upgrade process, use a Windows logon ID with Administrator authority.

About this task

To install the Administrative Command Line, complete the following steps:

Procedure
1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the folder that corresponds with your system. For example, there are folders that are labeled IA64, X64, and X86. In addition, there are folders for the various language packs.

3. Start the installation program.

4. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.

5. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. You must accept the terms of the license agreement to continue the installation.

6. A page is displayed prompting you to specify the target directory where the software is to be installed. Accept the default location that is displayed in the **Directory Name** field, or type over it to specify the location, or click **Browse** to go to the location. Click **Next**.

7. A page is displayed prompting you to select the **Installation Type**. Select **Advanced**.

8. Click **Next**.

9. Select **FastBack Administrative Command Line**. Following the list of features that you can select for installation, the space requirements are displayed.

10. Click **Next**.

11. If you are in a DHCP environment, enter either the IP address or the name of the FastBack Server (if your DHCP environment supports name registration). If your FastBack Server has a static IP address, enter either the IP address or the name of the FastBack Server. The FastBack Server name cannot contain a space.

12. Click **Next**.

13. The software is installed. To complete the installation, restart the system.

Results

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:

- Modify - Use this option to change the location of the installation.
- Remove - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing FastBack Mount
About this task

To install FastBack Mount, complete the following steps:

Procedure

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.

2. Go to the Tivoli Storage Manager FastBack folder that corresponds with your system architecture.

   - (Windows) Run the installation process with a Windows logon ID with Administrator authority.

   - (Linux only) Run the installation process as the root user. The root user profile must be sourced. If you use the **su** command to switch to root, use the **su -** command to source the root profile.

3. Start the installation program.

4. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.

5. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. You must accept the terms of the license agreement to continue the installation.

6. A page is displayed prompting you to specify the target directory where the software is to be installed. Accept the default location that is displayed in the **Directory Name** field, or type over it to specify the location, or click **Browse** to go to the location. Click **Next**.

7. A page is displayed prompting you to select the **Installation Type**. Select **Advanced**.

8. Click **Next**.

9. Select **FastBack Mount**. Following the list of features that you can select for installation, the space requirements are displayed.

10. Click **Next**.

11. If you are in a DHCP environment, enter either the IP address or the name of the FastBack Server (if your DHCP environment supports name registration). If your FastBack Server has a static IP address, enter either the IP address or the name of the FastBack Server. The FastBack Server name cannot contain a space.

12. Click **Next**.

13. The software is installed. To complete the installation, restart the system.

Results

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:

- `Modify` - Use this option to change the location of the installation.
- `Remove` - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing Central Control Station (Windows only)
About this task

To install Central Control Station, complete the following steps:

Procedure

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.

2. In the folder for Tivoli Storage Manager FastBack, go to the folder that corresponds with your system. For example, there are folders that are labeled IA64, X64, and X86. In addition, there are folders for the various language packs.

3. Start the installation program.

4. The welcome page is displayed. Click **Next**. The Software License Agreement page is displayed.

5. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. You must accept the terms of the license agreement to continue the installation.

6. A page is displayed prompting you to specify the target directory where the software is to be installed. Accept the default location that is displayed in the **Directory Name** field, or type over it to specify the location, or click **Browse** to go to the location. Click **Next**.

7. A page is displayed prompting you to select the **Installation Type**. Select **Advanced**.

8. Click **Next**.

9. Select **Central Control Station**. Following the list of features that you can select for installation, the space requirements are displayed.

10. Click **Next**.

11. If you are in a DHCP environment, enter either the IP address or the name of the FastBack Server (if your DHCP environment supports name registration). If your FastBack Server has a static IP address, enter either the IP address or the name of the FastBack Server. The FastBack Server name cannot contain a space. The name cannot contain a space.

12. Click **Next**.

13. The software is installed. To complete the installation, restart the system.

Results

If you start the executable file for the installation process after you complete the initial installation, a Program Maintenance window is displayed. From this window, there are two options:

- Modify - Use this option to change the location of the installation.
- Remove - Use this option to uninstall Tivoli Storage Manager FastBack.

Installing FastBack Reporting (Windows only)
Before you begin

Before you install FastBack Reporting, ensure that you meet all operating system, hardware, and software requirements. For more information about these requirements, see the topics in the Chapter 2, "Planning," on page 9 section.

About this task

To install FastBack Reporting, complete the following steps:

Procedure

1. Verify that all prerequisites are met. The following list identifies the prerequisites:
   - IBM Tivoli Common Reporting, Version 1.2 Fix Pack 1. You can download Tivoli Common Reporting, Version 1.2 Fix Pack 1 from the Passport Advantage online website at http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm. The installation instructions are online at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/ttcr_install.html.
   - FastBack Server, Version 6.1.0. For more information, see FB_InstallUse/FB_InstallUse/t_fast_install_fb_server.dita.
   - Web browser that is supported by Tivoli Common Reporting, Version 1.2 Fix Pack 1. For more information, see http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/ctcr_supported.html.

2. Start the executable file for FastBack Reporting: setup.exe.

3. The installation wizard window is displayed. On the Welcome page, click **Next**.

4. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. You must accept the terms of the license agreement to continue the installation.

5. A page is displayed prompting you to specify the destination folder where the FastBack Reporting is to be installed. Accept the default location, or click **Change** to go to the location. Click **Next**.

6. A confirmation page is displayed. Click **Install** to start the installation.

7. The installation process runs and a progress is displayed. When the installation process is complete, a page is displayed that confirms the installation completed. Click **Finish**. You can start the Tivoli Common Reporting Server. For instructions related to starting and configuring the Tivoli Common Reporting Server, see "Starting FastBack Reporting (Windows only)" on page 79.

Results

If you start the executable file for FastBack Reporting after you complete the initial installation process, a Program Maintenance window is displayed. From this window, there are two options:

- `Modify` - Use this option to change the location of the installation, or to delay the installation, or to disable FastBack Reporting.

- `Remove` - Use this option to uninstall FastBack Reporting.

Installing Tivoli Storage Manager FastBack with the console installation wizard (Linux only)

Using the console installation wizard is one method of installing Tivoli Storage Manager FastBack.

Before you begin

Important: (SELinux only) Before starting the console installation wizard, temporarily disable SELinux by entering the following command:

`/usr/sbin/setenforce 0`

About this task

To install Tivoli Storage Manager FastBack using the console installation wizard, complete the following steps:

Procedure

1. To start the wizard enter the following command:

   `./install-Linux.bin -i console`

   Note: If the installation is interrupted you can usually restart the installation process to continue the installation. However, if the installation fails to restart, a new, also known as clean, installation is required. To perform a clean installation you need to make sure that the product is fully removed before starting the installation process again. Enter the following commands to perform an clean installation:

   ```
   /ect/init.d/ioreporter stop
    /etc/init.d/FastBackClient stop
   cd /opt/IBM/Tivoli/TSM/FastBack/_uninst/TSM_FastBack
   ./Uninstall_IBM\ Tivoli\ Storage\ Manager\ FastBack
   rm /etc/init.d/FastBackClient
   rm /etc/init.d/ioreporter
   rm -rf /opt/IBM/Tivoli/TSM/FastBack/*
   rm ~/IA-FastBack-00.log
   ```

```
cd /tmp
rm -rf acsiTemp_root install.dir.*
/usr/ibm/common/acsi/bin/si_inst.sh -r -f
rm -fr /usr/ibm/common/acsi/logs/.lock*
./install-Linux.bin -i console
```

2. Follow the wizard directions, selecting **Next** to step through the wizard. You must accept the license agreement to complete the installation process.

3. On the summary page, if any errors are displayed, fix the errors. Information about the errors should be provided. The installation log file is stored in the following directory:

   `/opt/IBM/Tivoli/TSM/FastBack/`

   If no errors occurred, a message indicates that the installation is successful and a summary is provided.

4. Click **Done**.

What to do next

If you want to use a response file, the `FastBackInstaller.properties` file is provided. This documented response file is a file that you can edit and use. The following example shows the response file.

```
######################################################################
##
##  InstallAnywhere variable to configure for silent install
##
##   Usage:  install-{PLATFORM}.bin|exe -i silent -f <full path to this file>
##
##
######################################################################

#Has the license been accepted
#--------------------------  (uncomment the following line to accept the license)
LICENSE_ACCEPTED=TRUE

#----
#---- Choose Install Folder
#---- Silent Install :: Provide the fully qualified path. The default path is written below
#----

$USER_INSTALL_DIR$=/opt/IBM/Tivoli/TSM/FastBack


#----
#---- FastBack Server name
#---- Silent Install :: Provide the hostname for the FastBack Server
#----

#FastBack Server name
#-------------------
IAGLOBAL_HOSTNAME_CHECK=\"localhost\"


#----
#--- By default, the installer will install the FastBack Client and the documentation.
#--- To customize the silent installer uncomment the two lines below and set the
#--- variable CHOSEN_INSTALL_FEATURE_LIST to contain the features that you want to install.
#--- EXAMPLE ::  To install only the admin and server feature using
#---   the silent installer set the CHOSEN_INSTALL_SET and
#---   CHOSEN_INSTALL_FEATURE_LIST to the following values:
#---   CHOSEN_INSTALL_SET=Custom
#---   CHOSEN_INSTALL_FEATURE_LIST=FBClient,FBManager,FBMount,Docs
#--- Silent Install :: Remove the # from the front of all the lines and provide a list
#--- of features (separated by a comma) that you want to install. Do not install any extra space
#--- before or after the feature names.
#--- For a typical install (Client and documentation), leave the section below with comments.

CHOSEN_INSTALL_SET=Custom
CHOSEN_INSTALL_FEATURE_LIST=FBClient,FBManager,Docs
```

Installing Tivoli Storage Manager FastBack in silent mode

Running an installation in the background is one method of installing Tivoli Storage Manager FastBack. During this silent installation, no messages of any type are displayed. After the silent installation, upgrade, or uninstall process completes, you must restart the system.

Before you begin

The silent installation is supported for the following Tivoli Storage Manager FastBack components:
- FastBack Client
- FastBack Mount
- (Windows only) Administrative Command Line
- Documentation
- Central Control Station
- FastBack DR Hub Server
- FastBack Server
- FastBack data deduplication service
- FastBack Watchdog
- FastBack Disaster Recovery
- FastBack Manager
- License Agreement

For Windows systems, the silent upgrade and uninstallation processes work for all Tivoli Storage Manager FastBack components.

On Linux systems, the silent uninstallation process works for the FastBack Client and FastBack Mount components.

About this task

To silently install Tivoli Storage Manager FastBack on a supported Windows 32-bit operating system, complete the following steps:
1. Either download the code package or insert the Tivoli Storage Manager FastBack Product CD into the CD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the X86 folder.
3. In a text editor, open the `setup.iss` file.
4. Complete the following steps to edit the `setup.iss` file:
   a. Locate the line that starts with the following string:
      ```
      szDir=
      ```
   b. (Optional) If you are not using the default installation path, edit this line to reference the installation path that you are using.
   c. Locate the line that starts with the following string:
      ```
      SERVER_IP=
      ```
   d. Update the host name or IP address to reference the FastBack Server that you installed and are using.
   e. Save and close the `setup.iss` file.
5. From a command prompt window, enter the following command:
   ```
   setup.exe /s /f1"<path_to_the_setup.iss_file>"
   ```

6. Restart the system.

Note: The `setup.iss` file on the Tivoli Storage Manager FastBack Product CD is a sample file. It is necessary to record the `setup.iss` file for common use in silent mode. The recording is done by entering the following command:

```
setup.exe /r /f1"C:\setup.iss"
```

To silently install Tivoli Storage Manager FastBack on a supported Windows 64-bit operating system, complete one of the following procedures:

- To complete a clean installation in the default location, complete the following steps:
  1. Either download the code package or insert the Tivoli Storage Manager FastBack Product CD into the CD drive.
  2. In the folder for Tivoli Storage Manager FastBack, go to the X64 folder, or, for Itanium microprocessors, go to the IA64 folder.
  3. From a command prompt window, use the cd command to change directory to the installation folder
  4. Enter the following command:

     ```
     setup.exe /s /v/qn
     ```
  5. Restart the system.
- To complete a clean installation in a non-default location, complete the following steps:
  1. Either download the code package or insert the Tivoli Storage Manager FastBack Product CD into the CD drive.
  2. In the folder for Tivoli Storage Manager FastBack, go to the X64 folder, or, for Itanium microprocessors, go to the IA64 folder.
  3. From a command prompt window, use the cd command to change directory to the installation folder.
  4. Enter the following command:

     ```
     setup.exe /s /v"/qn INSTALLDIR=<your_installation_directory>"
     ```
  5. Restart the system.

To customize the components to install and the installation path, complete the following steps:

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product CD into the CD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the X64 folder, or, for Itanium microprocessors, go to the IA64 folder.
3. From a command prompt window, use the **cd** command to change directory to the installation folder.
4. Enter the following command:

   ```
   setup.exe /s /v"/qn INSTALLDIR=[installation_folder]
   ADDLOCAL= [Component]"
   ```

   Where [Component] is the part of the Tivoli Storage Manager FastBack product you want to install. You can install more than one component, and you must always install the license agreement.

   For example, if you want to install FastBack client, FastBack mount, and the license agreement, use the following command:

   ```
   setup.exe /s /v"/qn INSTALLDIR=[installation_folder]
   ADDLOCAL= client,mount,LAP"
   ```

The following table contains information about what [Component] to use in the command:

Component to install:	[Component] to use in the command:
FastBack Client	client
FastBack Mount	mount
Administrative Command Line	shell
Documentation	documents
Central Control Station	ccs
FastBack DR Hub Server	drserver
FastBack Server	server
FastBack Data Deduplication Service	storgenet
FastBack Watch Dog	watchdog
FastBack DR	DR
FastBack Manager	manager
License Agreement	LAP

5. Restart the system.

To silently install Tivoli Storage Manager FastBack on a supported Linux operating system, complete the following steps:

Tip: Before you start a silent installation, update the FastBackInstaller.properties file according to your requirements. Otherwise, only the FastBack Client is installed (by default).

Procedure
1. Download the code package or insert the Tivoli Storage Manager FastBack Product CD into the CD drive.
2. Go to the X86 folder. It is located within the Tivoli Storage Manager FastBack folder.
3. For the default installation, enter the following command into the command prompt window:

   `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true`
4. For a custom installation, enter the following command into the command prompt window:

   `./install-Linux.bin -i silent -f <full path to the FastBackInstaller.properties file>`
5. Restart the system.

What to do next

The Tivoli Storage Manager FastBack virtual volume is not installed during the installation process. This virtual volume is installed when FastBack Mount is started for the first time.

Installing the language packs

Tivoli Storage Manager FastBack supports installation of components on non-English versions of Windows, as well as non-ASCII objects (for example, host names, volume names, user names, passwords, and policies).

Before you begin

The language packs can be installed after Tivoli Storage Manager FastBack is installed. The language packs are available on the Product DVD.

About this task

To install a language pack on a supported Windows operating system, complete the following steps:

Procedure

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. Open a command prompt window and navigate to the DVD drive.
3. To start the language pack installation process, enter the following command (where *x* represents your DVD drive letter and *<lang>* represents the three-letter country code associated with that language):
   - (32-bit): *x*:\FastBack\LanguagePacks\Windows\LanguagePack_*<lang>*
   - (x64): *x*:\TSMFB\languages*<lang>*
4. Select **setup.exe** and click **OK**.
5. Follow the installation instructions contained in the prompt windows.
6. Click **Finish**.

What to do next

To install a language pack on a supported Linux operating system, complete the following steps:

1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. Open a command prompt window and navigate to the /media directory. For example, type the cd /media command.
3. Run the installation process. For example, type the ./cdrom/FastBack/ LanguagePacks/Linux/installLP-Linux.bin command. A Welcome page is displayed.
4. Follow the installation instructions contained in the prompt windows.
5. Click **Finish**.

Upgrading Tivoli Storage Manager FastBack

Administrator privileges are required to upgrade Tivoli Storage Manager FastBack. You must disconnect the FastBack Server system from the SAN until the FastBack Server upgrade is complete.

The upgrade process is the same for all Tivoli Storage Manager FastBack systems, including the server, client, and disaster recovery server computers.

Tivoli Storage Manager FastBack 6.1.7 supports upgrades from Tivoli Storage Manager FastBack version 6.1.5. If you must upgrade from an older version of FastBack, you must upgrade to version 6.1.5 first, and then upgrade to version 6.1.7.

To upgrade to Version 6.1.7, complete the following steps:

1. Download the code package.
2. Go to the folder where you saved the code package.
3. Start the upgrade process by running the `setup.exe` file.
4. A message is displayed. The message asks if you want to continue the upgrade process. Click **Yes**.
5. Another message is displayed with a progress indicator. The message and progress indicator provides the status of the upgrade process. When the upgrade process completes, click **Finish**.

The upgrade process completes and you can start using Tivoli Storage Manager FastBack. If you try to immediately start the FastBack Manager, the FBSG4302W message might be displayed. If this message is displayed, wait a few minutes before you start FastBack Manager.

Silent upgrade

To silently upgrade Tivoli Storage Manager FastBack on a supported 32-bit operating system, complete the following steps:
1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. Open the command prompt and use the cd command to change to the installation folder
3. Enter the following command:

   `setup.exe /s /f1" <path_to_the_upgrade.iss_file>"`
4. Restart the system.

Note: The `setup.iss` file on the Tivoli Storage Manager FastBack Product CD is a sample file. It is necessary to customize the `setup.iss` file before you install Tivoli Storage Manager FastBack in silent mode. This customization is done by entering the following command:

`setup.exe /r /f1"C:\setup.iss"`

To silently upgrade Tivoli Storage Manager FastBack on a supported 64-bit operating system, complete the following steps:
1. Either download the code package or insert the Tivoli Storage Manager FastBack Product DVD into the DVD drive.
2. In the folder for Tivoli Storage Manager FastBack, go to the `X64` folder, or, for Itanium microprocessors, go to the `IA64` folder.
3. From a command prompt window, enter the following command:

   `setup.exe /s /v"qn"`
4. Restart the system.

Upgrading Tivoli Storage Manager FastBack with the console installation wizard (Linux only)

Important: (SE Linux only) Before you start the console upgrade wizard, temporarily disable SE Linux by entering the following command:

`/usr/sbin/setenforce 0`

To upgrade Tivoli Storage Manager FastBack with the console upgrade wizard, complete the following steps:
1. To start the wizard, enter the following command:

```
./install-Linux.bin -i console
```

2. Select the local language and select **OK**.
3. Follow the wizard directions, selecting **Next** to step through the wizard. You must accept the license agreement to complete the upgrade process.

   Note:
   - The found installation directory window shows the installation directory and the installed components of the previous version.
   - The summary window shows the installation directory for the upgrade and the components to be upgraded.

4. Click **Done**

Uninstalling

You can use the following procedures to uninstall Tivoli Storage Manager FastBack. Before you remove Tivoli Storage Manager FastBack, you do not have to complete any steps to ensure that you do not lose your backup and archive data.

The uninstallation process is the same whether you completed a new installation or upgraded to this version of the software.

Note: A silent uninstall of Tivoli Storage Manager FastBack fails if it is being used to mount virtual volumes or to carry out an instant restore. Ensure that all instant restore processes are finished and that there are no virtual volumes that are mounted before you start a silent uninstall.

Uninstallation process for Windows operating systems

To uninstall Tivoli Storage Manager FastBack, use the standard `Uninstall` option in the Add or Remove Applications window, part of the Control Panel for the Windows operating system.

A rollback from Tivoli Storage Manager FastBack the current version to a previous version is not supported.

If a FastBack Server has read and write access to any non-repository SAN disk, the following steps must be completed:

1. After uninstalling FastBack Server, before rebooting, use LUN masking to disable access to the SAN disk from the FastBack Server.
2. Disconnect the system from the Fibre Channel.

If you do not complete these steps, the Windows operating system might cause disk corruption.

Formatting a disk that was used by the FastBack Server does not remove the FastBack repository bit. To clear the disk data and repository bit, remove the disk from the repository before you uninstall the FastBack Server. You can remove the disk by completing these tasks:

1. Open the Repository Pool view in the FastBack Manager GUI.
2. Right-mouse click the repository disk and select **Remove from repository**.

Restriction: A disk cannot be removed from a repository if it is the last disk or the only disk in the repository.

If you want to uninstall FastBack Reporting, complete the following steps:

1. Undeploy the history manager. To undeploy the history manager, complete the following steps:

    a. From the Windows Start menu, select **Programs** > **FastBack** > **Reporting** > **Withdraw History Manager**. A DOS command window displays the progress.

    b. During the withdraw history manager process, a window that requests logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password that is specified during the Tivoli Common Reporting installation process.

    c. Click **OK**.

    d. In the DOS command window, when the deployment history manager process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.

2. Delete the report package. To delete the report package, complete the following steps:

    a. From the Windows Start menu, select **Programs** > **FastBack** > **Reporting** > **Delete Report Package**.

    b. During the delete report package process, a window that requests logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password that is specified during the Tivoli Common Reporting installation process.

    c. Click **OK**.

    d. In the DOS command window, when the delete report package process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.

3. Start the executable file for FastBack Reporting: `setup.exe`.

4. Click **Next**.

5. A Program Maintenance window is displayed. From this window, there are two options:

    - `Modify` - Use this option to change the location of the installation, or to delay the installation, or to disable FastBack Reporting.

    - `Remove` - Use this option to uninstall FastBack Reporting.

    Select **Remove**.

6. Click **Next**.

7. Click **Remove**.

8. Click **Finish**.

To silently uninstall Tivoli Storage Manager FastBack on a supported Windows 32-bit operating system, complete the following steps:

1. In the installation directory for Tivoli Storage Manager FastBack, go to the `X86` folder.

2. From a command prompt window, use the cd command to change to the installation folder.

3. Enter the following command

   `setup.exe /s /f1"<path_to_the_uninstall.iss_file>"`
4. Restart the system.

Note: The `setup.iss` file on the Tivoli Storage Manager FastBack Product CD is a sample file. It is necessary to customize the `setup.iss` file before you install Tivoli Storage Manager FastBack in silent mode. The customization is done by entering the following command:

`setup.exe /r /f1"C:\setup.iss"`

To silently uninstall Tivoli Storage Manager FastBack on a supported Windows 64-bit operating system, complete the following steps:

1. In the installation directory for Tivoli Storage Manager FastBack, go to the `X64` folder, or, for Itanium microprocessors, go to the `IA64` folder.
2. From a command prompt window, enter the following command:

   `setup.exe /s /v"/qn REMOVE=ALL"`
3. Restart the system.

Uninstallation process for Linux operating systems

Run the uninstallation process as the root user. The root user profile must be sourced. If you use the **su** command to switch to root, use the **su -** command to source the root profile.

To uninstall Tivoli Storage Manager FastBack, complete the following steps:

1. Change to the directory for the uninstallation program. The following path is the default location to the uninstallation program: `/opt/IBM/Tivoli/TSM/FastBack/_uninst/TSM_FastBack`
2. Depending on the mode of installation, use one of the following methods to uninstall Tivoli Storage Manager FastBack:
   - To use the installation wizard to uninstall Tivoli Storage Manager FastBack, enter this command:

     `./Uninstall_IBM Tivoli Storage Manager FastBack`
   - To use the console to uninstall Tivoli Storage Manager FastBack, enter this command:

     `./Uninstall_IBM Tivoli Storage Manager FastBack -i console`
   - To silently uninstall Tivoli Storage Manager FastBack, enter this command

     `./Uninstall_IBM Tivoli Storage Manager FastBack -i silent`

Chapter 4. User management and security

With the correct user management definitions, the administrator can secure system access.

With Tivoli Storage Manager FastBack, the administrator can control user permissions by assigning users to user groups.

User groups are named, logical entities. You can assign permissions and users to user groups. There are two ways to set up user groups:

- Create and configured user groups in FastBack Manager. User groups that you create in FastBack Manager can have different access permissions. For example, one group might have administrator permissions and another group might have more restrictive permissions. To create and configure user groups, you must be classified as a `super user` with administrator permissions.

  Default user groups that are included with FastBack Manager cannot be changed.

- Use Microsoft Active Directory user groups that are added to the Active Directory group list in FastBack Manager. FastBack Manager recognizes these group members for the Active Directory as super users. These users are automatically assigned the correct access permissions.

There are some rules to follow when setting up user groups:

- A user can be assigned to only one user group.
- If you are the administrator, change the default password. Use the following rules when changing a password:
  - Passwords cannot match the user name.
  - Password must be at least 8 characters.
  - Passwords cannot exceed 20 characters.
  - Passwords must include at least one digit and one letter.
  - The following characters cannot be used: `\*?\"<>|;^'.$#@&,`

You can create new users or change existing users by using the Users and Groups window.

Configuring Active Directory groups

Active Directory groups are predefined groups of administrators with extensive system access permissions.

About this task

Use FastBack Server to use Active Directory groups as part of user login management. When you add an Active Directory group to the list, FastBack Manager recognizes members of this group during the logon process, and logs them as administrators.

When using the Active Directory group in a Global Group, the user and its associated group must be in the same Organization Unit. FastBack Manager cannot

recognize the members of a group when the user is a Super User. For example, if you create a Global Group named FB_GlobalGroup in Users O.U, you must also add the FB_GlobalGroup users to Users O.U.

If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the hotfix associated with this knowledge base article.

When using Active Directory with Microsoft Windows 2008, the FastBack Server needs to authenticate with the using a Domain Administrator account. To ensure that the FastBack Server service authenticates correctly, complete the following steps:
1. Log on to the FastBack Server
2. Click **Start** and then click **Run**
3. Type `services.msc` and click **OK**
4. Under Services, right-click the FastBack Server service and click **Properties**
5. Under the Log On tab, select This Account
6. Enter the Domain Administrator user name and password and click **OK**
7. Under Services, right-click the FastBack Server service and click **Restart**

To add an Active Directory group, complete the following steps:

Procedure
1. Go to **Configuration** > **General Configuration** > **Users and Groups**.
2. Right-click **Active Directory Groups**; then, click **New AD Group**.
3. In the displayed window, type the group name. The length of the group name cannot exceed 64 characters.
4. Click **Apply**.

Configuring FastBack Manager user groups

To simplify administration, minimize the number of user groups.

When planning user groups, the following items need to be considered:
- Who requires access to the FastBack Manager system?
- What tasks will the users complete?

When you know the answers to these questions, create the users and assign the users to user groups. When you create a user, immediately assign the user to a group.

Creating user groups

To create user groups, you must have administrator permissions.

About this task

To create a user group, complete the following steps:

Procedure
1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups**.

2. Right-click **Groups**; then, click **New group**.
3. Type the following information:
   - Group Name - Type up to 40 characters. Do not include trailing spaces.
   - Description - Type a description to characterize the user group.
4. Click **Apply**.

Results

You entered all the information required to create the user group. You can add users to and associate permissions with the group.

Assigning permissions
About this task

To assign permission to a user group, complete the following steps:

Procedure
1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups** > **Groups**.
2. Select a group.
3. In the User Group window, click **Show Permissions**.
4. Select the permissions that you want to assign. There are two permissions you can select:

   Administrator privileges
   > Use to configure client groups, job schedules, and policies. Users with administrator privileges can change options for general configuration.

   Restore Disks and Volumes
   > Use to restore volumes for one or more servers.

5. Click **Apply**.

Assigning users
A user can belong to only one user group.

There are two ways you can assign a user to a user group:
- Use the User Group window to transfer an available user to the selected members list.
- Use the User window to choose a user group from a list.

To assign a user to a user group with the User Group window, complete the following steps:
1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups** > **Groups**.
2. Select a group.
3. In the User Group window, select the available users that you want to transfer to the selected members list and move the users.
4. Click **Apply**.

To assign a user to a user group with the User window, complete the following steps:
1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups** > **Users**.

2. Select a user.
3. Select a user group for the user.
4. Click **Apply**.

Creating users

To create users, you must have administrator permissions.

About this task

To create a user, complete the following steps:

Procedure

1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups**.
2. Right-click **Users**; then, click **New user**. The default properties for the user are displayed.
3. In the right-pane, type the following required information:
   - User Name: The name that you want the user to type when logging on to the FastBack Manager system. You can use a name with up to 24 characters; do not include trailing spaces.
   - Password: The password that you initially assign to the user. Use the following rules when assigning a password:
     - Passwords cannot match the user name.
     - Password must be at least 8 characters.
     - Passwords cannot exceed 20 characters.
     - Passwords must include at least one digit and one letter.
     - The following characters cannot be used: *?\"<>|;^'.$#@&,

     Users can change their passwords. Users with administrator permissions can change passwords for other users.
   - Confirm Password: A confirmation of the password you typed in the previous field.
4. (Optional) For the user description, type descriptive information about the user. For example, you can type a job title, department, or organization name.
5. Select a user group. The default user group is *LimitedGroup*. Users must be assigned to a user group. To view the properties of the selected user group, click **View Group**.

Changing user properties

All changes take effect immediately, regardless of whether the user ID is logged in or logged out.

About this task

If you log in and, while the credentials are authenticated, your user ID is disabled, you can use Tivoli Storage Manager FastBack until you log off. The disabled user ID cannot be used to log on again.

To change the properties for a user, complete the following steps:

Procedure

1. Select the user from the tree.
2. In the right-pane, change the properties.

   The following properties can be changed:
   - User name
   - Password
   - Description
   - User group
3. Click **Apply**.

Deleting users

Deletions are effective immediately, unless the user being deleted is logged on to the system. In this case, when the deleted user logs out, the user is deleted.

About this task

The administrator user cannot be deleted. To delete a user, complete the following steps:

Procedure

1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups** > **Users**.
2. Right-click the user that you want to delete; then, click **Remove**. A message is displayed to confirm the deletion. Click **Yes** to delete the user group or **No** to cancel the deletion and leave the user group intact.

What to do next

To delete all users, complete the following steps:

1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups**.
2. Right-click **Users**; then, click **Reset users**. This action resets the user list to the default set of users. In the default set of users, there is one user. This user is the administrator.
3. A message is displayed to confirm the deletion. Click **Yes** to delete all users or **No** to cancel the deletion.

Changing user group properties

Changes to user group properties are effective immediately.

About this task

To change the properties of a user group, complete the following steps:

Procedure

1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups** > **Groups**.
2. Select a group.
3. Change the properties as needed.

   The following properties can be changed:

- Name and description
- Assigned permissions
- Assigned users
4. Click **Apply**.

Deleting user groups

To delete users, you must have administrator permissions. You cannot delete the default user groups: `LimitedGroup`, `ADLimitedUsersGroup`, and `SuperAdminGroup`.

About this task

To delete a user group, complete the following steps:

Procedure

1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups**.
2. Right click the user group that you want to delete; then, click **Remove**.
3. When the system prompts you to confirm the deletion, click **Yes** to delete the user group. Click **No** to cancel the deletion and leave the user group intact.

What to do next

To delete all user groups, complete the following steps:

1. In the FastBack Manager Configuration tab, go to **General Configuration** > **Users and Groups**.
2. Right-click **Groups**; then, click **Reset Groups to Default**.
3. When the system prompts you to confirm the deletion, click **Yes** to start the operation or click **No** to cancel the deletion.

Access permissions

Access permissions give specific groups of users authorization to access source and destination volumes.

Volume restore

Volume restore can be implemented only if the currently logged user is authorized to access both the source and the destination volume.

SuperAdmin users are given restore access to all domains. These *SuperAdmin* users can be either Microsoft Active Directory users, or FastBack Manager domain users who belong to the *SuperAdmin* group.

Users that are not administrators require read permissions, Share and ACL, to the source volume root directory, and Modify permissions, network share and ACL, to the destination volume root directory. The source permissions were in effect when the backup was implemented, while the destination permissions are the current permissions during restore.

If a volume restore is attempted to or from a location where the logged user does not have access permissions, a message is posted in the status bar for FastBack Manager.
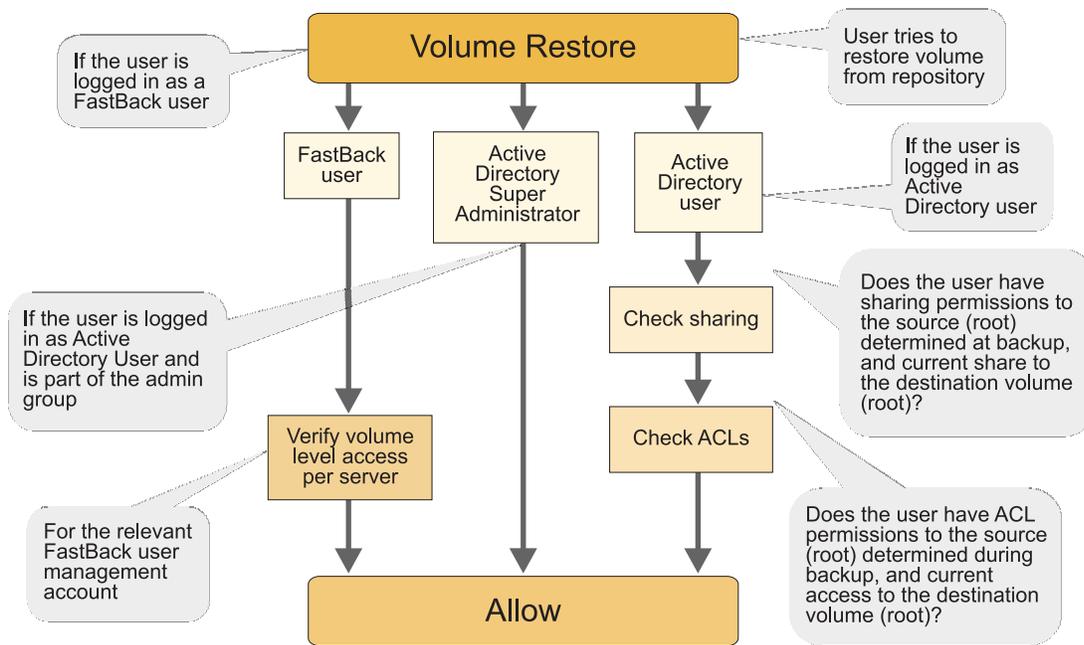
Figure 5. Volume Restore Access Privileges

instant restore (Windows only)

instant restore can be run from source volumes to destination volumes that the current user is authorized to access.

SuperAdmin users have unlimited restore rights. These *SuperAdmin* users can be either Active Directory users, or *Xpress-Restore* domain users belong to the *SuperAdmin* group.

Active Directory users that are not administrators require read permissions for sharing to the source volume root directory, and change permissions (ACL) to the destination volume root directory. The source permissions are granted at backup time, while the destination permissions are granted at restore time.
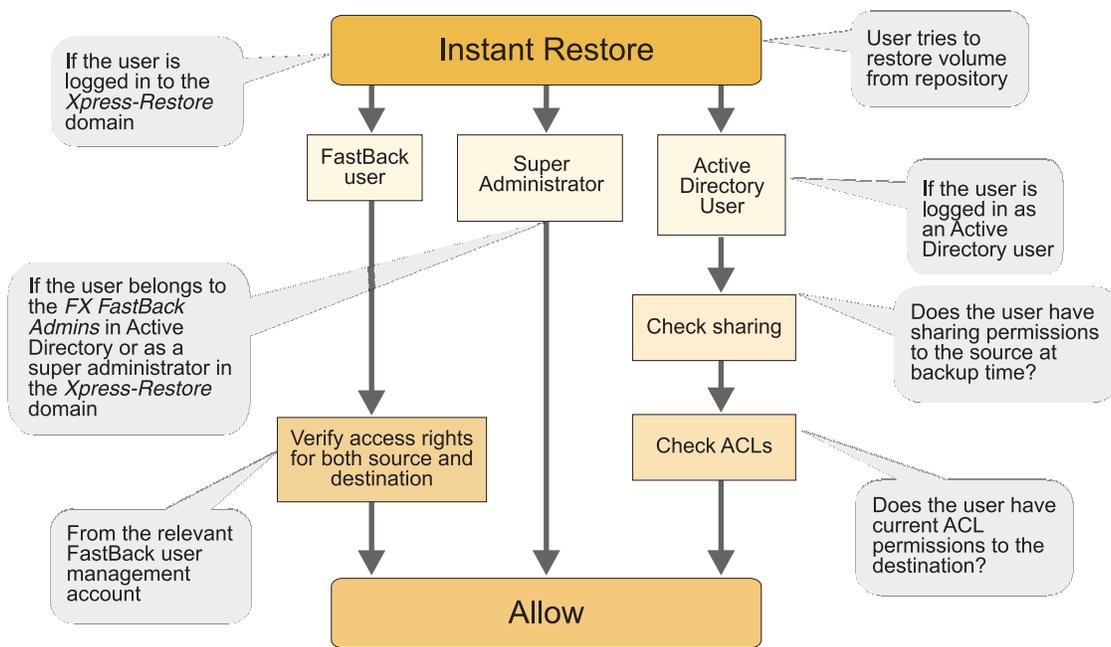
Figure 6. instant restore access privileges

Source permissions are checked for only local and SAN repositories.

Security and login

Tivoli Storage Manager FastBack provides two distinct security mechanisms: Microsoft Active Directory accounts and Tivoli Storage Manager FastBack local accounts. The security mechanisms are defined by different domains, users, and permissions. Different users can be logged-in simultaneously using different types of accounts, but a single user cannot combine permissions from Active Directory and Tivoli Storage Manager FastBack accounts.

By default, the FastBack Manager is accessed through the current Active Directory access privileges. The user can log off and log on again at any time, and use any domain and any user name allocated to that domain.

Administrator privileges can be granted only to a user from the domain of the system. The *AD group* cannot be added from a domain other than the domain you are logged into.

Note: To use FastBack Manager, the user that is logged into the FastBack Manager system must be a member of the Administrators user group. Alternatively, the user must have write permissions to the following folder: `C:\Program Files\Tivoli\TSM\FastBack\Manager`

Tivoli Storage Manager FastBack dual security provides significant advantages as follows:
- Integration with the organization directory. Because new users and groups do not have to be defined specifically for Tivoli Storage Manager FastBack, there is no additional administrative usage.
- Simplified access. FastBack Manager is accessed directly and the Windows login permissions for the user are applied.

- Redundancy. If the Active Directory for the organization is unavailable, access mechanism for the FastBack Manager can be used to secure access.

Active Directory integration

Active Directory is a directory structure that is integrated in Windows 2000 and later that controls account management security. It enables a user to log on to computers and domains with an identity, which is given access privileges to domain resources. This operation is done through the Access Control Lists (ACL). The ACLs are a set of data that are associated with a file, directory, or other resource. The ACLs define the permissions that users and groups have for accessing that resource. In the Active Directory service, an ACL is a list of access control entries that are stored with the object it protects.

Share level and file level security information that are associated with a specific volume, folder, or file of the original volume, is used to restore file, volume, and disk.

When the Active Directory group in a Global Group is used, the user and its associated group must be in the same Organization Unit. FastBack Manager cannot recognize the members of a group when the user is a Super User. For example, if you create a Global Group named `FB_GlobalGroup` in Users `O.U`, you must also add the `FB_GlobalGroup` users to Users `O.U`.

If the login domain account does not have the share or file level permissions that are required to access a specific file or volume, one can log off and log on again, using an account with the required privileges, to acquire restore permissions.

When you use the Active Directory with Microsoft Windows 2008, the FastBack Server needs to authenticate by using a Domain Administrator account. To ensure that the FastBack Server service authenticates correctly, complete the following steps:

1. Log on to the FastBack Server
2. Click **Start** and then click **Run**
3. Type `services.msc` and click **OK**
4. Under Services, right-click the FastBack Server service and click **Properties**
5. Under the Log On tab, select This Account
6. Enter the Domain Administrator user name and password and click **OK**
7. Under Services, right-click the FastBack Server service and click **Restart**

Note: In Windows 2000, Active Directory users can open different domains and still use the same user name without reentering the password. In Windows 2003, the user is prompted to reenter the user name and user ID password every time a new domain is being accessed.

Microsoft Active Directory user in the FastBack Manager

Active Directory groups are predefined groups of administrators with extensive system access privileges. You can use the FastBack Server to use these groups as part of user login management. When you add an Active Directory group to the Active Directory group list, in FastBack Manager (see "Configuring Active Directory groups" on page 67), FastBack Manager recognizes members of this group during logon, and log the users on as administrators. After installation, the set of Microsoft Active Directory groups is empty. Adding and removing Active Directory groups to and from the Microsoft Active Directory group list in FastBack

Manager requires superuser access privileges. To configure Microsoft Active Directory groups, the first-time user must have Tivoli Storage Manager FastBack superuser privileges.

For non-administrator users that are not members of an Active Directory group, the non-administrator users can view only the configuration options, monitor snapshots, and restore volumes, folders, and files to which they have access permissions on the network.

Tivoli Storage Manager FastBack accounts

FastBack Manager accounts are created with the FastBack Manager. Two default groups are provided: *LimitedGroup* and *SuperAdminGroup* members are assigned all the administrative and restore permissions for the *XPRESS-RESTORE* domain.

Tivoli Storage Manager FastBack users

The user names and user groups in this special domain are unrelated to the users or groups defined in the Microsoft Active Directory, even if some of the assigned users or groups have the same names. User privileges are determined only by the definitions assigned to the FastBack Manager group to which they are allocated.

Switching between Tivoli Storage Manager FastBack and Active Directory domains

For volume restore, switch between accounts by logging off and then on again.

FastBack Manager login with using a different user name
About this task

Use this option to log in with a different user name for volume-level restores.

Procedure
1. From the FastBack Manager File menu, choose **Login as...** and respond to the verification dialog by clicking **Yes**.
2. Select the **Domain**. To enter the Tivoli Storage Manager FastBack environment, select the *Xpress-Restore* domain and enter the **User Name** and **Password**. To enter an Active Directory domain, select the appropriate domain and enter a User Name and Password defined in that domain.
3. Click **Login**. If a difference is detected between the time on the FastBack Server clock and the management console clock, you are prompted to synchronize the clock according to your console before the FastBack Manager window is displayed. See "Setting the system clock" on page 90, for additional information about setting the system clock.

Securing the FastBack Server application data directory
About this task

The user is responsible for securing the application data directory for FastBack Server, located in the Documents and Settings section for the user. The security of the system is not guaranteed if the FastBack Server application data directory is not properly secured, for example, in case the application data directory for the FastBack Server is shared through sharing of the C: disk on the network.

Chapter 5. Starting and configuring

This section provides instructions for how to start and configure the Tivoli Storage Manager FastBack software, and how to navigate the FastBack Manager.

Configuring Tivoli Storage Manager FastBack

The following list summarizes the configuration tasks for Tivoli Storage Manager FastBack:

1. (Optional) Change connection parameters to the FastBack Server.
2. Verify that the FastBack Server clock is set to match the system clock.

Starting and running services for Tivoli Storage Manager FastBack

By default, when you start the operating system, the services for Tivoli Storage Manager FastBack are started.

(Windows only) The Tivoli Storage Manager FastBack services include FastBack Server, FastBack Client, FastBack DR Hub Server, FastBack Mount, FastBack data deduplication, and FastBack Watchdog. These services are started under the Local System Account.

If you experience a malfunction and suspect that the problem might be caused by incorrect authorization, you can run the problematic service from an account that has more privileges. For example, you can log on as a Local or Domain administrator. You can stop and restart the services by using the Windows Services window. To locate the Services window, go to the Control Panel. Go to **Administrative Tools** > **Services**.

(Windows 2008 and Vista only) When you start FastBack Mount from the Microsoft Windows Start menu, the service is automatically stopped. You can use the Windows Services window to start the FastBack Mount service. To locate the Services window, go to the Control Panel. Go to **Administrative Tools** > **Services**.

In addition, when the FastBack Mount user interface is closed, the FastBack Mount service is restarted. You can use the Windows Services window to stop the service.

(Linux only) The only Tivoli Storage Manager FastBack services that run on supported Linux operating systems are FastBack Client and FastBack Mount. These services run as the root user. You can start, stop, and query the services by using the following commands:

Start client
> `/etc/init.d/FastBackClient start`

Stop client
> `/etc/init.d/FastBackClient stop`

Query client status
> `/etc/init.d/FastBackClient status`

Note: A FastBack Server with more than one Linux client computer connected to it might restart automatically if the FastBack Client service is stopped on any of the Linux client computers that are connected to the FastBack Server.

Starting FastBack Manager

Before you begin

(Windows only) Installing the FastBack Server and FastBack Client on the same system is supported. However, if you install the server and client on the same system, before you start FastBack Manager, enable the `SAN Module` option. When you install the FastBack Client, by default, the `SAN Module` option is disabled. For more information about enabling the `SAN Module` option, see "Connecting client to server" on page 87.

About this task

To start FastBack Manager, complete the following steps:

Procedure

1. Use one of the following procedures:
   - (Windows only) From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Manager**.
   - (Linux only) From the Linux client, complete the following steps:
     a. Change the current directory to the following directory:
        `<install_directory>`/manager

        The default `<install_directory>` path is `/opt/IBM/Tivoli/TSM/FastBack/`
     b. Run the following command:
        `./manager/fastbackmanager.sh`
     c. Enter the FastBack Server IP address.
2. In the login window, type your user name. The default user name is *admin*. The authorization policy is case-sensitive. Letters must be typed in the correct case.
3. Type your password. The default password is *admin123*. The authorization policy is case-sensitive. Letters must be typed in the correct case.
4. Select a domain. The default domain is *XPRESS-RESTORE*. After you select the domain, the configuration is loaded.
5. Click **Login**. A message is displayed.

   If this is the first time you start the FastBack Manager, you can click **Add Repository** to identify a repository. If you do not want to identify a repository, click **Cancel**.

   After FastBack Manager is displayed, you can add a repository by selecting **General Configuration** > **Storage Pool** > **Repository Pool**. From the menu, you can add or claim a repository. For more information, including details about the maximum volume size, see "Add Repository wizard" on page 98.

   For more information about configuring and using Tivoli Storage Manager FastBack, see Chapter 6, "Backing up and restoring," on page 91.

Results

If the FastBack Manager does not connect to the FastBack Server and the FastBack Server is running on a system that is part of an Active Directory domain, complete the following steps:

1. Change the Active Directory settings to allow for anonymous enumeration SID and name translations.
2. Log off.

3. Log on.

4. Restart the FastBack Server service.

5. Grant the FastBack Server service administrative rights by changing the *logon as* properties for the FastBack Server service to an Active Directory administrator account.

Starting FastBack Reporting (Windows only)

After you install FastBack Reporting, you are to complete several tasks before you can start FastBack Reporting.

Before you begin

Before you start FastBack Reporting, complete the following steps:

1. Start the Tivoli Common Reporting Server. To start the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Server**.

2. Configure FastBack Reporting. To configure FastBack Reporting, complete the following steps:

   a. Deploy the history manager. To deploy the history manager, complete the following steps:

      1) From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **Reporting** > **Deploy History Manager**. A DOS command window displays the progress.

      2) During the deploy history manager process, a window that requests logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password that is specified during the Tivoli Common Reporting installation process.

      3) Click **OK**.

      4) In the DOS command window, when the deploy history manager process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.

      5) If the reporting server is a x64 server, run the following command: `FastBackShell.exe -c set_connection server_computer FB_SERVER_NAME`

      By default, the history manager loads history data every hour (3600 seconds). This configuration parameter is set in the `config.properties` file. The default path to the file follows: `C:\Program Files\Tivoli\TSM\ FastBack\reporting\conf\config.properties`

      The variable is *HISTORY_INTERVAL*. The default parameter is *3600*. The range is from *600* seconds (10 minutes) to *31536000* seconds (365 days).

   b. Import the report package. To import the report package, complete the following steps:

      1) From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **Reporting** > **Import Report Package**. A DOS command window is opened and displays the progress.

      2) During the import report package process, a window that requests logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and

password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password that is specified during the Tivoli Common Reporting installation process.

   3) Click **OK**.

   4) In the DOS command window, when the import report package process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.

   c. Configure FastBack Manager to access the Tivoli Common Reporting Server. To configure FastBack Manager access to the Tivoli Common Reporting Server, complete the following steps:

   1) From the **Configuration** tab, select **General Configuration**.

   2) In the main window, select the **Reporting** tab.

   3) Type the host name or IP address for the Tivoli Common Reporting Server.

   4) Type the port number for the Tivoli Common Reporting Server. By default, the Tivoli Common Reporting Server uses port *16316*.

   5) Click **Apply**.

3. Stop the Tivoli Common Reporting Server. To stop the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Stop Tivoli Common Reporting Server**.

4. Start the Tivoli Common Reporting Server. To start the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Server**.

About this task

To start FastBack Reporting, complete the following steps:

Procedure

1. From the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Browser**.

2. In the browser window, a message displays a warning about the website security certificate. Continue to the website.

3. Type the user ID and password you set during the Tivoli Common Reporting installation process. The default user name is *tipadmin*. Use the password that is specified during the Tivoli Common Reporting installation process.

4. Click **Log in**.

5. In the navigation pane, click the **+** icon next to **Reporting** to expand the tree. An entry for `Common Reporting` is displayed.

6. Select **Common Reporting**.

7. In the navigation pane, click the **+** icon next to **Report Sets** to expand the tree.

8. In the navigation pane, click the **+** icon next to **Tivoli Products** to expand the tree.

9. In the navigation pane, select **FastBack Reporting**.

What to do next

After you start FastBack Reporting, if you use the default installation directory, you run reports. For instructions related to running and viewing reports, see "Running and viewing reports (Windows only)" on page 191.

However, if you change the default installation location (for example, if you change `C:\ProgramFiles\Tivoli\TSM\FastBack\Reporting` to `D:\ProgramFiles\ Tivoli\TSM\FastBack`), configure the data source before you run reports. For instructions related to configuring the data source, see "Configuring the data source (Windows only)" on page 190.

Navigating FastBack Manager

The FastBack Manager main window provides three tabs:

- Configuration tab - Use to set general options, user management, and snapshot scheduling configuration options.
- Snapshots Monitor tab - Use to monitor the status of past and currently running snapshots according to user-selected filters, providing links to all restore options.
- Recovery tab - Use to set restore options. Access to the available options depends on the user privileges.

Toolbar icons are provided for common operations. The status bar at the bottom of the main window provides information about the system connection and repository capacity.

Toolbar icons

Table 19. Toolbar icons

Toolbar icons	Description
	Starts the wizard selection menu. Wizards guide the user through the creation of policies at various levels.
	Adds another object according to the currently selected category or element.
	Removes the currently selected object.
	Opens the FastBack Server log view.
	If you installed FastBack Reporting, this icon is enabled. The icon opens a browser window for Tivoli Common Reports.
	Displays the help window.

Status bar icons

When the FastBack Server is in a busy state, FastBack Manager attempts to reconnect. Until FastBack Manager connects to FastBack Server, FastBack Manager remains in a *read-only* mode and access to options is limited.

Table 20. Status bar icons

Status bar icons	Description
	Connected to network, data transfer in progress.

Table 20. Status bar icons (continued)

Status bar icons	Description
	Connected to network, but no data transfer is in progress.
	Disconnected from network.
	Repository detected, but no activity is carried out on the repository. For example, snapshots or cleanup operations are not running.
	Repository capacity OK and repository operation is in progress.
	Repository not detected, or the repository space reached the defined limits.
	Clean up operations in progress.
	Snapshot or cleanup policies in progress.
	One of the defined primary storage devices is not detected.
	No activities currently in progress on the primary storage.
	Disk layout is being updated.
	Connection OK.
	Connection to the FastBack Server lost.
	Version problem.
	FastBack Server is busy.
	Disaster recovery status.

Configuration

The Configuration tab provides all the system configuration and operation categories and functions. These include administrative functions such as user groups and security levels for specific users, repository configuration and management, and all functions related to backup definitions.

The Configuration window has two vertically divided panes. You can select configuration categories from the tree in the navigation pane. The main window area displays the options corresponding to the selected category.

You can right-click to select a category or object in the tree. A pop-up menu displays options relevant to the selection.

Configuration tree options

The following entries are available from the Configuration tab navigation tree:

- General Configuration - FastBack Server connection parameters, clean up, and global parameters

- Storage Pool - Summary of disks and volumes attached to the FastBack Server and each backed up client
- Users and Groups - User and group authentications and permissions
- Client Groups - Definitions of volumes to be snapped
- Job Schedules - Backup schedules management options
- Policies - Snapshot policies consist of selected Client Groups and the associated Job Schedules
- Pending Jobs - Jobs in queue
- FastBack Server Log - Displays system-related events
- FastBack status - Status

Configuration icons

The following icons might be used on the Configuration tab.

Table 21. Icons that might be used on the Configuration tab

Toolbar icons	Description
	General configuration
	Users
	Groups
	FastBack Client
	Disconnected FastBack Client
	FastBack Client is not responding to FastBack Server connection attempts
	FastBack Client has incompatible version
	Job schedules
	Pending jobs
	Job paused
	Policy paused
	Policies
	Policy
	FastBack Server log
	Client groups
	Warning
	SAN disk (basic, dynamic, unknown)

Table 21. Icons that might be used on the Configuration tab (continued)

Toolbar icons	Description
	Information
	Repository disk
	Repository enabled for data deduplication
	Repository enabled for data deduplication is backing up data
	Repository enabled for data deduplication reports a problem
	Repository enabled for data deduplication is retaining data
	Warning for the repository enabled for data deduplication
	Error or alert
	DAS disk
	Cluster DAS disk
	Cluster SAN disk
	Disaster recovery
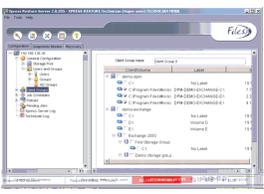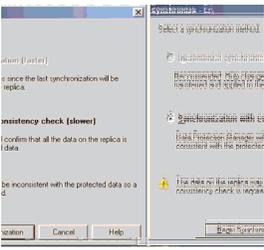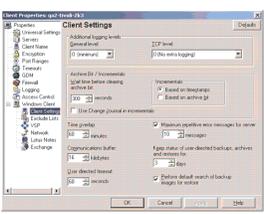
Snapshots Monitor

You can use the Snapshots Monitor tab to monitor the status and properties of snapshots. Use the tab to start various actions on the displayed snapshots and the respective snapshot chains. These include snapshots that are completed, either successfully or unsuccessfully, and snapshots that are in progress.

This window has two panes: a pane that provides filter options and another pane that displays the snapshots according to the selected filter criteria. When a category, for example, State or Date, is selected, the relevant options become available under the category. You can use these options to identify and filter the snapshots that are displayed in the monitor according to various criteria.

In the snapshot display pane, on the right side of the window, an additional menu can be displayed by right-clicking on a selected snapshot. The menu options vary, depending on the type of snapshot. For example, an *Aborted* snapshot would provide only the following options: Events, Erase, and Snapshot Properties. When you select the Erase option, you can erase all selected snapshots.

Right-click to select a snapshot. From the pop-up menu, you can start snapshot-related tasks and view snapshot properties.

Retry policy

When the execution of a snapshot fails, the snapshot is marked as *Aborted* with a yellow exclamation mark.

Tivoli Storage Manager FastBack attempts to run the snapshot again for the number of times specified in the policy setup. When the snapshot runs, the snapshot is marked as *Running*. If the snapshot fails to complete within the specified number of retries, it is marked as *Aborted* with a red exclamation mark after the last retry.

Table 22. Snapshot icons

Toolbar icons	Description
	Initializing or running snapshot
	Continuous data protection snapshot is running
	Snapshot completed successfully
	Continuous data protection Snapshot completed successfully
	Successful snapshots whose retention time expired
	Aborted Continuous Data Protection snapshot, the Continuous Data Protection data before the aborting point might be available.
	Aborted snapshots
	Aborted snapshots whose retention time expired
	Successful snapshot that was detected as unreliable

Table 22. Snapshot icons (continued)

Toolbar icons	Description
	Successful CDP that was detected as unreliable
	Successful snapshot but CDP aborted and detected as unreliable
	Successful snapshot and detected as unreliable (Displays in technician mode only)
	Successful snapshot detected as unreliable before generation (Displays in technician mode only)

For more information about setting the number of retries to recover from a failed snapshot attempt, see "Error recovery: Setting the number of retries" on page 181.

Recovery

The Recovery tab, part of the FastBack Manager window, provides access to all restore options.

Access to specific options is limited by access rights of specific users. To access FastBack Mount from this tab, FastBack Mount must be installed on the same system as the FastBack Manager.

The Recovery tab provides the following options:

- **Volume Level Restore** - Use for restoration of entire volumes.
- **Disk Restore** - Creates a disk from snapshots of several volumes. The disk can be either a SAN or DAS disk. DAS disks with a boot and system designated volume are not supported. For these types of DAS disks, Tivoli Storage Manager FastBack for Bare Machine Recovery can be used.
- **FastBack Mount and Instant Restore** - Enables mounting snapshots and instant restore of volumes for disaster recovery purposes.

  instant restore works only with mounted volumes (volumes that are assigned a drive letter).

Handling multiple LAN cards on the same computer

Having two LAN cards on the same computer can result in identification and communication problems. This situation can prevent the FastBack Server and FastBack Client from communicating properly.

To resolve these communication problems, only one LAN card is to be registered in the DNS server. The entries of other LAN cards of the same computer are to be removed from the DNS server. After you complete these tasks, you are able to connect a FastBack Client to a FastBack Server.

(Windows only) To remove a LAN card entry from the DNS server, complete the following steps from the Network Connections Control Panel:

1. Choose a primary LAN card.
2. Right click the non-primary LAN card; then, click **Properties** > **General**.
3. From the displayed list, select **Internet Protocol - TCP/IP**.
4. Click **Properties**.

5. Enter a static IP address, and click **Advanced**. The Advanced TCP/IP Settings dialog is displayed.

6. Select the **DNS** tab.

7. Clear the **Register this connection's addresses in DNS** box, which is towards the bottom of the **DNS** tab display.

8. Ask your system administrator to help you locate the DNS server for your system.

9. In the DNS server, locate your computer, and delete your computer entry line in the DNS server.

10. Go to **Run** > **cmd**.

11. Type **ipconfig /flushdns**. This command flushes the DNS entry from the DNS cache for the client.

Connecting client to server

About this task

(Linux only) To connect a FastBack Client to a FastBack Server, complete the following steps:

1. In a text editor, open the `FastBackClient.ini` file. The default location for this file is `/opt/IBM/Tivoli/TSM/FastBack/client/var`.

2. In the [HOSTNAMES] section, add either the host name or IP address for the server. After the @ character, enter for a new line. Add a tab before the IP address. For example:

```
[HOSTNAMES]
IP-Adrs-List @
 192.168.1.110
```

3. Save the `FastBackClient.ini` file.

4. Restart the FastBack Client.

(Linux only) If the FastBack Client backs up SAN disks, complete the following steps:

1. In a text editor, open the `FastBackClient.ini` file. The default location for this file is `/opt/IBM/Tivoli/TSM/FastBack/client/var`.

2. In the [SAN module] section, set the **SAN enabled** value to *1*. For example:

```
[SAN module]
SAN enabled = 1
```

3. Save the `FastBackClient.ini` file.

4. Restart the FastBack Client.

(Windows only) You can use the FastBack Client Configurator to connect a client to a FastBack Server. To start and use the FastBack Client Configurator, complete the following steps:

Procedure

1. On the system where the FastBack Client is installed, from the **Start** menu, choose **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Client Configurator**.

2. Verify the host name or IP address for the FastBack Server.

3. (Optional) If you have a cluster environment, enable the SAN Module option.

   This setting is required for a cluster environment, because, when nodes switch, incremental delta block snapshots are required. In a cluster environment, every

local disk at each node is to have a different disk signature. For example, if *disk1* on *node1* has the same signature as *disk1* on *node2*, an error might occur.

4. Click **OK**.

Configuration and log files

Configuration files are needed for Tivoli Storage Manager FastBack to run correctly, but is not to be edited. Do not edit any of the configuration files. Log files are used by IBM technical support to diagnose problems that affect Tivoli Storage Manager FastBack.

(Windows only) FastBack data deduplication errors are not written to the FastBack Server or other Tivoli Storage Manager FastBack component log files. For information about the FastBack data deduplication service errors, reference the Windows Event log.

(Windows only) For Microsoft Windows operating systems, the default location for the log files is *user_home*\tivoli\tsm\fastback\manager\log, where *user_home* is the path to the documents and settings folder of the user. In this path, there are subdirectories with a folder for each Tivoli Storage Manager FastBack service. For example, there are folders labeled mount, shell, client, and server. The log files are named according to the Tivoli Storage Manager FastBack service. For example:

c:\Documents and Settings\tivoli\tsm\fastback\manager\log

(Linux only) The default location for the FastBack Manager log files is *user_home*/tivoli/tsm/fastback/manager/log. For example:

/root/tivoli/tsm/fastback/mount/log

The default location for the FastBack Client log files is /opt/IBM/Tivoli/TSM/FastBack/client/var.

The log file format is .sf. In addition, each log file is assigned a number. For example, *FAST_BACK_CLIENT040.sf*.

The log file with the most recent data is stored in the log file with the *040* number. When a log file reaches the maximum size limit, a new log file is created. The log file name is the same except that the log file number decrements by one. Specifically, the data in the log file with the *040* number is copied to a log file with the *039* number. The log file with the *040* number contains the newest log file data. When *040* again reaches maximum file size, the *039* file contents move to *038* and the *040* information goes to *039* again.

Changing connection parameters to FastBack Server

Administrator privileges are required to change the connection parameters used to connect to FastBack Server.

In the following scenarios, changes in connection parameters might be required:

- If the current connection is not available when the FastBack Manager is started, you are prompted to enter the IP address or name of an FastBack Server. Type the entry and click **Connect**.

  If the FastBack Server runs on the Windows XP operating system, you need to change the default Windows firewall setting from *on* to *off*.

- If the connection becomes unavailable while using the FastBack Manager, you can type the IP address or FastBack Server computer name in the **General Configuration** > **General** tab. Type the IP address or name, and click **Connect**.

Working with FastBack Manager in WAN environment

When working with FastBack Manager in a WAN environment, connect to the FastBack Server by IP address and not by name.

(Windows only) If you used the default installation directory, the `FastBackManager.ini` file is stored in the following directory: `C:\Program Files\Tivoli\TSM\FastBack\manager\`

(Linux only) If you used the default installation directory, the `FastBackManager.ini` file is stored in the following directory: `/opt/IBM/Tivoli/TSM/FastBack/manager/`

Related overview information about WAN environments is available in "Using data deduplication in a wide area network" on page 5.

Configuring SAN environment

The World Wide Name (WWN) of the FastBack Server HBA card must be obtained to open LUN masking. Reference your HBA documentation for instructions.

About this task

To configure a LUN, complete the following steps:

Procedure

1. LUN masking must be enabled for the disks on which the repository is configured.
2. If the LUN Management utility supports read/write configuration masking, **Write** mode must be enabled for the Repository disks on the FastBack Server system only. Other systems are to have *Read Only* access to the repository disks.
3. LUN masking must be enabled on all disks that are to be backed up.
4. If the LUN Management Utility supports read and write configuration masking, enable *Read Only* access for FastBack Server to disks that are to be backed up.
5. SAN zoning must be enabled on:
   - The switch
   - All disks to be backed up
   - The FastBack Server
   - The server clients
6. The target disk for restored volumes must have LUN masking, and be write-enabled.

What to do next

If there are SAN repository disks in the network, access to these disks is to be restricted to a system that has either FastBack Server or FastBack Mount installed. FastBack Server must be able to access the repository in read and write mode. FastBack Mount is to have access to the repository in read-only mode, however, FastBack Mount can access to the repository in read and write mode.

Setting the system clock

Verify that the FastBack Server clock is set correctly because all backup and restore operations are referenced according to this clock.

About this task

Clock changes require resetting the FastBack Server. Examples of when you reset the system clock and need to reset the FastBack Server include the following items:

- Time synchronization of the Windows clock with the domain controller
- Change of time zone configuration
- Daylight savings time change

Each time that you start FastBack Manager, the system verifies that the time on the FastBack Server clock and the clock on the system the FastBack Manager is installed on is the same. If a significant difference is detected, you are prompted to synchronize the values.

To prevent changes in the clock from affecting job schedules and labeling, all currently running jobs are cancelled when a reset is run on the FastBack Server. When the FastBack Server restarts, the jobs start automatically.

In most circumstances, the FastBack Server time is updated according to the system clock time. If the FastBack Server time does not match the system clock time, a reset of the FastBack Server is required.

Chapter 6. Backing up and restoring

The following scenario is a common usage scenario for Tivoli Storage Manager FastBack:

Step 1: Identify a repository.
A repository is the disk area used for storing client snapshots. The FastBack Server uses the repository. The repository can be a folder, a physical disk, a SAN, or NAS drive. Before you can use Tivoli Storage Manager FastBack, at least one repository must be defined.

Note: When you add a repository by using VMware ESX virtual guest or Microsoft Hyper-V virtual guest, use either a folder or volume for the repository. Other types of repositories cannot be added when using VMware ESX virtual guest or Microsoft Hyper-V virtual guest.

For more information about identifying repositories, see "Repositories" on page 93.

Step 2: Schedule and run snapshots.
A snapshot is a record of backup data at a certain point in time. To schedule and run snapshots, you must create a client group, job schedule, and snapshot policy. A snapshot policy links one or more client groups to a job schedule.

There are several types of snapshots:

- Full: This type of snapshot is a complete image of the used part of the volume. A full snapshot is the first snapshot in every chain. For the maximum number of simultaneous full snapshots, the default is *3* simultaneous snapshots. Incremental delta block and checkpoint snapshots are counted as full snapshots. The default value, *3*, must not be changed.

- Incremental: Instead of taking a complete image of the volume, the incremental snapshot takes only the data that changed since the last snapshot.

  In some situations, the incremental snapshot is interrupted. When an incremental snapshot is interrupted, one of the following scenarios occurs after the interruption:

  - An incremental delta block snapshot starts. An incremental delta block snapshot starts because at least one of the following conditions is met:

    - An unexpected system shutdown.
    - A device is unexpectedly removed from the system. For example, if a cable is disconnected for a SAN disk while the client system is operational and an incremental snapshot is in progress.
    - When the system volume is not on the first disk (disk 0), all disks on this machine start an incremental delta block snapshot.
    - The system is part of a cluster.
    - When the Application Data folder is not on the system volume, all disks on this machine start an incremental delta block snapshot.

  - If the conditions in the previous item are not met, and a normal system shutdown occurred, the incremental snapshot restarts.

- Incremental delta block: This type of snapshot calculates the differences between the last successful snapshot in a chain, and the actual data on the disk. This type of snapshot cannot be manually set, but you can request this type of snapshot when you initiate a checkpoint snapshot. The incremental delta block snapshot is taken in the following scenarios:
  - The client system is restarted after a power or system failure. An example of a system failure is an unexpected shutdown.
  - The client service is restarted and it is more than seven days since the last delta block snapshot.
  - The client service is inactive. A delta block snapshot does not always occur when the client service becomes active after a period of inactivity. The software determines whether to run a delta block snapshot based on the amount of input/output on the system and the amount of time when the client service was inactive.
  - In an error recovery scenario when the client and server do not identify the same snapshot as the base snapshot. If the client and server systems identify different snapshots as the base snapshot, the next snapshot is a delta block snapshot, not an incremental snapshot.

  Incremental delta block snapshots occupy as much disk space as the incremental snapshots, but the time required to perform the incremental delta block is similar to the time required to complete a full snapshot.

- Checkpoint: A checkpoint snapshot is the same as an incremental delta block snapshot with one minor difference. The difference is that you can start a checkpoint snapshot from FastBack Manager. An incremental delta block snapshot cannot be started from FastBack Manager.

For more information about scheduling and running snapshots, see "Setting up snapshot policies" on page 106.

Step 3: For critical servers, run Continuous Data Protection.
Continuous Data Protection is a tool that records all activity between snapshots, allowing the restoration of a system to a point in time. Using Continuous Data Protection requires additional processor, memory, and network bandwidth resources. Because of these additional requirements, do not run Continuous Data Protection on volumes where page files or the operating system files are installed.

For more information about running Continuous Data Protection, see "Continuous Data Protection (Windows only)" on page 141.

Step 4: Recover data.
With the snapshots that are stored on the FastBack Server, you can recover data that is backed up. There are several ways to recover data:

- Recover volumes. For more information about recovering volumes, see "Restoring volumes" on page 126.
- instant restore with FastBack Mount. For more information about instant restore, see "Instant Restore (Windows)" on page 129 or "File-level restore and instant restore (Linux)" on page 134.
- Recover files. For more information about recovering files, see "Recovering files" on page 127.

During the cleanup process, FastBack Server detects snapshots that are potentially corrupted. When FastBack Server detects a potentially corrupted file, a warning message is displayed and a message is written to the FastBack Server log. During the next scheduled snapshot of the volume a job is run to repair the snapshot. You must not use a potentially

corrupted snapshot. If a problem occurs and you need the data before the repair job for the snapshot completes, complete the following steps:

1. Run the file system check tool. You can see the operating system documentation for more help in completing this step.

2. Run the application consistency check tool. You can see the operating system documentation for more help in completing this step.

Step 5: Recover data from applications and databases.

You can use Tivoli Storage Manager FastBack to back up data from applications, for example, Microsoft Exchange server, and databases, for example, Microsoft SQL Server.

For more information about recovering data from applications and databases, see the following sections:

- For recovering Microsoft Exchange data, see "Microsoft Exchange back up and restore" on page 146.
- For recovering Microsoft SQL Server data, see "SQL backup and restore" on page 153.
- For recovering Lotus Domino® database data, see "Backing up and restoring Lotus Domino Databases" on page 160.
- For recovering DB2 UDB database data, see "Backing up and restoring DB2 UDB databases" on page 167.

Step 6: Recover operating system partitions from an uncorrupted system.

You can use Disk Restore from the Recovery window to restore a physical server to a virtual or temporary server while a physical server is replaced or repaired.

For more information about recovering operating system partitions from an uncorrupted system, see "Recovering operating system partitions by using Disk Restore" on page 171.

Repositories

A repository is an area used by FastBack Server to store client snapshots. The repository can be a folder, a volume, a physical disk, on local disk drives, or a SAN or NAS drive.

For your first repository, you can use a folder, volume, or disk. If you use a folder-based repository, make sure that this reserved space is always available and not used by Windows files or data. In addition, ensure that anti-virus software and defragmentation tools do not run on the disk or volume that are holding the contents of the repository.

Before you can use Tivoli Storage Manager FastBack, at least one repository must be defined. Do not use a system disk as a repository. A folder, volume, or disk that is not identified as the system disk is to be used as a repository.

While using a system disk as a repository is not prohibited by the software, using a system disk is not advised. System disks typically have an operating system partition and other open files and applications that are running. When using a system disk for a repository, it must be defined as a repository folder on disk. The system disk cannot be defined as a repository disk volume. When defined as a repository folder on disk, the system administrator must make sure that the free space allocated exists and is never used up by other applications or the operating system.

When creating a repository to back up data in a production environment, plan at minimum for the repository to store three times the size of the used space on the servers that are being backed up. The preferred size of the repository is five times the size of the used space on the servers that are being backed up. You can use the following space to record your size needs.

```
(Size of volumes being backed up) x 3 = _____ Minimum FastBack Server
repository size


(Size of volumes being backed up) x 5 = _____ Preferred FastBack Server
repository size
```

If you use the Add Repository Wizard to add a disk to the repository, you can select to add the entire disk to the repository, and FastBack Manager opens the disk for read/write access so you do not have to use the disk open utility. (Specifically, you want to add the entire disk, not the larger volume, or a partition on the disk, to the repository.) If you do not add the entire disk to the repository, any drive you attach to the FastBack Server needs to be opened for read/write privileges before being used. You can use the disk open utility to help with this task. For more information about using the disk open utility, see "Allowing read/write access to a disk with disk open utility" on page 102.

FastBack Server supports a mix of repository types. Only the FastBack Server is to be writing to the disk, volume, and share. The repositories that you identify are organized into a group called a storage pool.

Storage pool

A storage pool is a system disk-management utility for managing disks and the volumes that the disks contain. To create and manage repositories, and monitor the storage layout, you can use options from the storage pool menus.

All disk-related tasks are done without shutting down the system or interrupting users. Most configuration changes take effect immediately.

Note: Tivoli Storage Manager FastBack runs automatic discovery to continuously update the display. However, if you suspect that the display requires updating, you can run a manual refresh by selecting Storage Pool; then, right-click to select **Rescan Volume Layout**.

Types of repositories

The following table sums up the advantages and disadvantages of using different location types for backup images.

Location	Advantages	Disadvantages
Local hard drive	• Stand-alone, dedicated storage for images • Can detect file system corruption and recovery • Inexpensive • Fast, when compared to network disks • Accurate capacity management • Central management	• Vulnerable, no fault tolerance • A dedicated disk is required • Only Microsoft basic disks are supported

SAN storage	• Fast • Fault tolerant • Managed • Can detect file system corruption and recovery • Instant recovery over the SAN by any system connected to the SAN • Accurate capacity management • Central management	• Expensive
Network storage	• Storage diagnostic - NAS or any network location	• Appropriate accesses rights must be assigned • Capacity management is not accurate • No detection of file system corruption or failure • No central management
Volume or folder	• Flexibility, no need for special dedicated disk	• No accurate capacity management • No central management • Must be large enough to hold snapshot (full or incremental) • A large number of volumes and folders can harm the restore and recovery performance

When you create a repository using a volume or folder, you can choose to use the repository for data deduplication. If you have a repository that is using data deduplication and you want to disable data deduplication, remove the repository. Create a repository and do not enable data deduplication. You cannot use a data deduplication repository and a standard repository interchangeably.

Repository pool

Repository disks and volumes can be grouped and organized into a repository pool. There is one repository pool per FastBack Server. A repository pool is associated with a storage pool.

Before creating repositories

The FastBack Server repository can be composed of, at most, 20 disks. Examples of disks include a physical disk, LUN, volume, or NAS unit.

Before you add a disk to the repository, read the following information:
- For a volume, the size must not exceed 16 TB.
- For a disk, the size should not be equal to or greater than 2 TB
- Disks must not be scanned by a virus scanner.
- Disks or volumes that have open files or running applications cannot be assigned.
- An object that was selected as part of a repository cannot be backed up.
- If you assign a folder, you must ensure that the size allocated reflects the free space available on the volume. The FastBack Server software does not verify that there is sufficient free space.

- The system administrator must make sure that the local system account on the FastBack Server has access privileges to the network share that contains the repository folder.
- A volume chosen for the repository must be formatted as NTFS only.

Disks that are in use, also known as mounted, cannot be added to repositories. If, when you add a disk to a repository, a volume letter is not automatically assigned, manually assign a volume letter.

When you add a disk that is not shared on the network to the repository, the repository works, but instant restore is not possible unless you install FastBack Mount on the same system as the FastBack Server. If you do not want to install FastBack Mount and FastBack Server on the same system, but need to use instant restore for the repository, share the disk on the network and add the disk to the repository.

Unclaimed repositories: Unclaimed repositories are FastBack repository disks that are visible to the FastBack Server but are not owned by the FastBack Server. Unclaimed repositories exist as a result of either of the following situations:
- A new FastBack Server installation was completed on an environment that previously contained FastBack repository disks.
- An existing repository is maintained for use by a newly installed FastBack Server to retrieve old data.

Unclaimed repositories are visible in the FastBack Manager GUI **Storage Pool**. An unclaimed repository is available for use as a repository for the current FastBack Server. The user can claim such a repository in the FastBack Manager, but only if it is the first repository of the FastBack Server. After claiming such a repository, the FastBack Server discovers and manages the snapshots in that repository. The FastBack Server does not function without an assigned repository. Even when unclaimed repositories are visible to the FastBack Server, an unclaimed repository or a new repository must be assigned.

A folder must be empty when it is added to the repository.

Assigning access privileges for Active Directory
Tivoli Storage Manager FastBack, FastBack Mount must be assigned access privileges of an existing Active Directory member to access shared repository objects on the network.

About this task

To assign access privileges of an existing Active Directory member for Tivoli Storage Manager FastBack, complete the following steps:

Procedure
1. Go to **General Configuration > Remote Repository Access** tab.
2. Type the user name and password of an existing Active Directory member that has full access rights to the repository.
3. Click **Apply**. It takes 10 minutes for the new settings to be updated. FastBack Server uses this information to access shared repository objects on the network.
4. Test Tivoli Storage Manager FastBack network repository access.

What to do next

To assign access privileges of an existing Active Directory member for FastBack Mount, complete the following steps:

1. In the **FastBack Manager**, click the **Configuration** tab. The Configuration window appears.
2. In the tree, select **General Configuration**.
3. In the main window, click the **FastBack Mount Access** tab.
4. Select **Assign FastBack Mount access to repository**.
5. Select the domain for an Active Directory member. This domain is used by FastBack Mount to access the repository.
6. Type a user or group name. The user or group name must have full access rights to the repository.
7. Select **Show FastBack Mount repository access reminder message** to not assign repository access to FastBack Mount, but want to be reminded to complete this task.
8. Click **Apply**. It takes 10 minutes for the new settings to be updated.
9. Test FastBack Mount network repository access.

Identifying DAS and SAN disks

Before you identify a DAS or SAN disk, install FastBack Mount or FastBack Server. By default, when you install FastBack Server, FastBack Mount is also installed.

After you install the Tivoli Storage Manager FastBack software, when creating a repository or adding to an existing repository, you can assign a SAN disk. To assign a SAN disk, use the Assign signature wizard that is part of the Microsoft Windows operating system. If you use the Assign signature wizard without FastBack Mount or FastBack Server installed, the repository disk that is taken over by that server can become corrupted.

- A SAN disk is seen as a DAS disk to the FastBack Server in the following situations:
  - The disk is under LUN Masking and was enabled to a protected system, but not enabled to the FastBack Server.
  - The disk is connected to a different SAN Island than the FastBack Server.
  - The Fibre Channel cable of the FastBack Server is disconnected.
  - The disk is owned by Microsoft cluster.
  - FastBack Server and FastBack Client see the same SAN disks, but FastBack Client has a disabled SAN module.
- A DAS disk is added to the storage layout only if during the connection of the client the volume is not seen through the SAN. However, a DAS can become a SAN device. For example, you can reconnect the Fibre Channel cable.
- If a volume is not available, a snapshot is not scheduled for that volume.

Creating repositories

When you add a volume, folder, or disk to the repository, the entire object is used by Tivoli Storage Manager FastBack. In addition, when you add a disk or partition, Tivoli Storage Manager FastBack reformats the disk or partition. All data is erased. You cannot add a disk that is equal to or greater than 2 TB, and it should not be scanned by any virus scanning tool. When creating a deduplication repository in

an environment that is protected by a firewall, TCP port 48879 must be opened on the firewall. The deduplication repository must be on a local volume or folder and cannot be on remote storage.

The repository can be created with one of the following methods:
- Adding repository space by using a wizard. Use this method for adding network shared folders to the repository.
- Adding volumes or folders to the repository.
- Selecting and adding a disk to the repository.

Attention: (Windows 2008 only) When you create a repository on a disk, the following message might be displayed:

```
You need to format the disk in drive x before you can use it.
Do you  want to format it?
[Format disk] [Cancel].
```

Click **Cancel** to ignore and dismiss the message. If you click **Format Disk**, data loss can occur. In addition, you cannot create policies or take new snapshots.

When you create a repository using a volume or folder, you can choose to use the repository for data deduplication. If you have a repository that uses data deduplication and you want to disable data deduplication, remove the repository. Create a repository and do not enable data deduplication.

If a disk was a Tivoli Storage Manager FastBack repository for a FastBack Server, you cannot add it as a repository to a different FastBack Server. The disk must be reformatted. After reformatting the disk, you can add the repository as a new, blank disk to the FastBack Server.

If you add repository space to the repository pool or if you add a complete disk to the repository after the FastBack server was installed, you must use the disk open utility unless the disk is already open. The disk open utility is a program that was developed to establish read/write privileges to a physical disk after FastBack Server is installed. After you install FastBack Server, any drive you attach to the FastBack Server needs to be opened for read/write privileges before being used. For more information about using the disk open utility, see "Allowing read/write access to a disk with disk open utility" on page 102.

Note: A folder must be empty when it is added to the repository.

Add Repository wizard

Use the Add Repository Wizard to detect and add potential disks or volumes on the server to the repository pool. If no repository is identified, the Add Repository Wizard is displayed.

If you use the Add Repository Wizard to add a disk to the repository, you can select to add the entire disk to the repository. Since FastBack Manager opens the disk for read/write access, you do not have to use the disk open utility. (Specifically, you want to add the entire disk, not the larger volume, or a partition on the disk, to the repository.) If the entire disk is not added to the repository, any drive you attach to the FastBack Server needs to be opened for read/write privileges before being used. You can use the disk open utility to help with this task. For more information about using the disk open utility, see "Allowing read/write access to a disk with disk open utility" on page 102.

When you create a repository by using a volume or folder, you can choose to use the repository for data deduplication. If you have a repository that uses data deduplication and you want to disable data deduplication, remove the repository. Create a repository and do not enable data deduplication.

To start the Add Repository Wizard, complete the following steps:

1. From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Manager**.
2. In the logon window, type your user name. The default user name is *admin*.
3. Type your password. The default password is *admin123*.
4. Select a domain. The default domain is *XPRESS-RESTORE*. After you select the domain, the configuration is loaded. This process might take a few minutes. You cannot click **Login** until the configuration is loaded.
5. Click **Login**.
6. In the dialog window, click **Add Repository** to start the Add Repository Wizard. The wizard scans the server and lists the disks and volumes. Only empty disks and volumes can be selected and defined as new repositories.

   If a dialog window is not displayed, open FastBack Manager and select **General Configuration** > **Storage Pool** > **Repository**. Right-click on Repository in the tree; then, click **Add Repository**.
7. Select the disk or volume that you want to add as a repository.
8. (Optional) If you select a volume to add as the repository and no other disk, volume, or folder has a repository assigned to it, you can select **Use repository for data deduplication**.
9. Click **Apply**.

   Attention: (Windows 2008 only) When you add a repository on a disk, the following message might be displayed:

   ```
   You need to format the disk in drive x before you can use it.
   Do you  want to format it?
   [Format disk] [Cancel]
   ```

   Click **Cancel** to ignore and dismiss the message. If you click **Format Disk**, data loss can occur. In addition, you cannot create policies or take new snapshots.

Note: When adding a disk to a repository, the disk size must not be equal to or greater than 2 TB. If you need a repository size equal to or greater than 2TB, you need to create a repository as a volume or folder. If you add a disk that is equal to or greater than 2 TB in size to a repository, an error occurs. To work around the error, complete the following steps:

1. Uninstall FastBack Server.
2. Remove the FastBack Server configuration files. The default location for these files is in the `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack` path.
3. Restart the system.
4. Use the Windows disk management tool to create a 1.99 TB primary partition volume on the disk.
5. Create a folder on that volume. For example, `E:\FastBackRep1`.
6. Install FastBack Server.
7. Identify the volumes you created in step 4 to FastBack Server with the Add Repository Space option. For more information about adding repository space, see "Adding volumes or folders to the repository" on page 100.

8. After you click **Apply** to close the Add Repository Space window, select the **Detect FS Corruption** option.
9. Click **Apply**.

Adding volumes or folders to the repository

The term *volume* means a discrete unit of storage on disks. When using Tivoli Storage Manager FastBack and adding volumes to a repository, the term *volume* is equivalent to the entire disk. No other data can be on the volume or the FastBack Server does not allow the volume to be added.

Before you begin

Note: Adding space to a FastBack Server repository that is enabled for data deduplication is not supported. You can add space to a repository not used for data deduplication.

When selecting a folder to be used as a repository, size constraints are to be considered when creating a repository for Tivoli Storage Manager FastBack. Take the size of the disk, subtract the existing data size from the disk size that might exist on the drive, and enter a size for the repository that does not exceed the available free space on the disk. For example, if you have a 32 GB drive and 18 GB of space is used, you have 14 GB of available space that can be used by FastBack Server as a repository.

Tivoli Storage Manager FastBack does not track when the disk is full. Even if no space is available, Tivoli Storage Manager FastBack tries to copy data to the repository.

If the root directory folder is an unused volume on a remote server, add a root directory folder of a data volume to the repository.

Note: A folder must be empty when it is added to the repository.

If you need to add repository space that is on a shared volume over the network, you must change the logon credentials from *Local System* to *Administrator*. To change the logon credentials, complete the following steps:
1. From the Windows Start menu, select **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click to select the FastBack Server service; then, click **Properties**.
3. In the Properties window, go to the Log On tab.
4. In the **Log on as** list, select **This Account**.
5. Enter the administrator account and authenticate with the domain controller.
6. Click **OK**.

About this task

To add volumes or folders to the repository, complete the following steps:

Procedure
1. Go to the Configuration tab and select **General Configuration** > **Storage Pool** > **Repository Pool**. Right click a storage pool; then, click **Repository Pool**.
2. Right-click to select a repository pool; then, click **Add Repository Space**.

3. The path to the folder is to be in the complete network path format (UNC format). Either type in a path in UNC format, or click the button next to the **Path** field and select the required disk.

4. Type the size you want to allocate for the repository to use on that volume. Tivoli Storage Manager FastBack does not monitor when the disk is full. Type a size that is reasonably less than the capacity of the drive. For example, you can allocate 16 GB on a 19 GB partition.

5. (Optional) Clear the **Detect FS corruption** checkbox to exit limited mode. Exiting limited mode might take up to 10 minutes.

   By default, **Detect FS corruption** is selected. When selected, this setting means that when a file system is corrupted, the system automatically enters limited mode. For more information about limited mode and suggested recovery, see "Limited mode" on page 185.

6. Click **Apply**.

Selecting and adding a disk to the repository
Procedure

1. In the Configuration pane, click **General Configuration**.

2. Select **Storage Pool**. The list of storage devices attached to systems with FastBack Server and SAN disks, along with some basic attributes, are displayed according to volumes and disks.

3. For each disk to be added to the repository, right-click the disk that you want to add; then, click **Add to Repository**. The disks already assigned to the

   repository are indicated by the ![icon] icon.

4. If the disk you want to add to the repository includes partitions or is a dynamic disk, a message window is displayed. The message warns that all data on the selected disk is destroyed if you decide to proceed with the operation. The disk is formatted with the NTFS file system. While the repository is being formatted, a message is displayed in the status bar. When the operation is complete, the disk icon changes to indicate that the disk is a repository.

   Attention: (Windows 2008 only) When you add a repository on a disk, the following message might be displayed:

   ```
   You need to format the disk in drive x before you can use it.
   Do you  want to format it?
   [Format disk] [Cancel]
   ```

   Click **Cancel** to ignore and dismiss the message. If you click **Format Disk**, data loss can occur. In addition, you cannot create policies or take new snapshots.

Creating a repository on a different domain
About this task

To add a repository on a domain other than the local domain, complete the following steps:

Procedure

1. Add a small local repository. For more information, see "Add Repository wizard" on page 98.

2. Use the following steps to set a user name and password:
   - Go to **General configuration** > **Remote Repository Access** tab.
   - Use the following format to enter the domain and user name: *domain\user name*.

- Enter a password.
- Click **Apply**. Applying the new settings can take as many as 10 minutes.

3. Add the new repository on the desired domain.

4. After you create the repository on a different domain, remove the small repository you created on the local domain.

Allowing read/write access to a disk with disk open utility

After you install FastBack Server, the disk write protection feature is automatically enabled. Before you use any drive that you attach to the FastBack Server, the drive is to be opened for read and write privileges. By default, disks that are added have read-only privileges.

If disk open is not used after you attach a new drive to the FastBack Server, any time you try to write data to the drive, all data goes to the buffer. It might seem that data is being copied to the drive, but, if you restart the server, the data is gone because the data was not physically written to the drive. Depending on the amount of data that is written to the disk, you might see some errors reported by the system. For example, "Delayed Write Failed" error messages are logged in the Windows system event logs. Another side effect includes the failure to initialize and format new disks.

The disk open utility must be run from the command line. The disk open utility can take the disk number of the respective disk that you want to open for read/write privileges as an argument. You can find the disk number in the Windows Disk Management window. The disk open utility also takes the DisableSANProtection and EnableWriteOnAllConnectedDisks arguments that are shown.

You can use disk open in the following scenarios:

- If you do not use the FastBack Server SAN mode, for example, LAN-free backup and SAN backup, you can use diskopen to disable the disk write protection feature. The following steps disable the FastBack Server SAN disk write protection. After you complete these steps, all disks are accessible for read and write operations.
  1. From the Microsoft Windows Start menu, select **Start** > **Run**. Enter the following command:

     `CMD`
  2. In the command prompt window, change to the directory that contains the **diskopen** tool. The default directory is `C:\Program Files\Tivoli\TSM\ FastBack\utilities`.
  3. Enter the following command:

     `DiskOpen -DisableSANProtection`
  4. Restart the system if prompted by the disk open utility.

  After you restart the server, all existing and newly connected disks are accessible for read and write operations.

- If you use the FastBack Server SAN mode, for example, LAN-free backup and SAN backup, you can use diskopen to open new disks that are connected to the FastBack Server. The following steps enable read and write access to all connected disks. Any new disk that is connected to the FastBack Server, after you complete the following procedure, is write-protected.
  1. Disconnect the shared SAN disks from the FastBack Server.

> **Attention:** Completing the following steps when the shared SAN disks are connected might cause irreparable disk damage that results in data loss.

2. From the Microsoft Windows Start menu, select **Start** > **Run**. Enter the following command:

   ```
   CMD
   ```

3. In the command prompt window, change to the directory that contains the **diskopen** tool. The default directory is `C:\Program Files\Tivoli\TSM\FastBack\utilities`.

4. Enter the following command:

   ```
   DiskOpen -EnableWriteOnAllConnectedDisks
   ```

5. Restart the system if prompted by the disk open utility.

Changing repository pool properties

You can change the properties for the repository pool.

About this task

To change the repository pool properties, complete the following steps:

Procedure

1. On the Configuration tab, expand **General Configuration**.
2. Expand **Storage pool**.
3. Select **Repository Pool**.
4. In the main window, a table displays information about the repositories. Right-click a row in the table to select it, and then click **Edit**.
5. As needed, change the following properties:

   > Folders and volumes - Size, and description. The path is displayed and cannot be changed.

   > Disks - Description.

6. Click **OK**.

Repository capacity

You can control the repository usage through the Cleanup tab.

If the repository fills to its capacity, the next snapshot attempt fails and the system notifies the user that new snapshots cannot be taken. In that case, add a repository or erase chains with the Snapshots Monitor view.

In addition, the repository usage alert field in the **General Configuration** > **Maintenance** tab defines the critical repository usage threshold. When this threshold is reached, the **Repository Status** field, in the status bar at the bottom of the window, turns red. In addition, a warning is logged in to the FastBack Server log. If the repository usage keeps growing, the message is logged again each time the level increases by 5 percent.

To keep the repository within the set limit, an immediate cleanup can be run or the cleanup scheduler can be set. The **Maintenance** tab also provides a way to schedule a cleanup task for the repository. Click **Run now** for an immediate cleanup. You can also click **Cleanup scheduler** to schedule cleanups. For more information about setting up the cleanup process, see "Defining cleanup parameters" on page 178.

You can also configure the software to send a periodic email alert to notify
recipients about the repository space thresholds.

Viewing storage pools

To view storage pools, open FastBack Manager.

In the main window, on the Configuration tab, expand **General Configuration** >
Storage Pool. The Storage Pool window is displayed. The Storage Pool window is
divided into two adjacent panes: the upper pane provides a volume-based storage
view and the lower pane provides a disk-based storage view. A bar separates the
two panes. The relative size of the panes can be changed by clicking and holding
down the left mouse button on the bar. Drag the bar up or down to resize the
panes.

Each type of storage pool is assigned an icon. The following table identifies the
icons that can be displayed.

Table 23. Storage pool icons

Storage pool icons	Description
	SAN disk. Backed up by the FastBack Server through the SAN.
	DAS (Direct Attached Storage). Backed up by the FastBack Server through the LAN.
	Identified as an Tivoli Storage Manager FastBack repository disk. If the capacity is displayed, it belongs to the connected FastBack Server; otherwise it belongs to a different FastBack Server.
	Repository on folder.

Viewing volume properties for storage pools

Basic information is available for each volume.

To view the information, right-click the volume in the Storage Pool window and
select **Properties**.

Label   Volume Name

File System
> File restore system (NTFS)

Capacity
> Volume capacity

Type   Basic - Not managed by any volume management software.

> Dynamic - Managed by a volume management software.

> Unknown - Not identified by Tivoli Storage Manager FastBack. For
> example, AIX® formatting.

Signature
> Volume signature

Viewing disk properties for storage pools

Basic information is available for each disk.

To see the disk properties, right-click the disk in the Storage Pool window and select **Properties.**

Name   Disk name.

Physical name
Disk specification for manufacturer.

Signature
Disk signature.

Type   Basic- Not managed by any volume management software.

Dynamic - Managed by volume management software.

Unknown - Not identified by Tivoli Storage Manager FastBack. For example, AIX formatting.

Capacity
Disk capacity

Block size
Block size

Simultaneous
Number of simultaneous reads or writes

Rate (MB per second)
Read and write rate

Setting priority for storage pools:

You can control the computer resources used by FastBack Client when you set client priority.

About this task

The FastBack Client uses system resources, for example, memory, disk, and network bandwidth, as needed, until a threshold is reached. The FastBack Client might use more resources than is specified by the priority level. If resource usage exceeds the threshold, the usage is reduced by terminating snapshots and freeing resources used by the snapshots.

Procedure
1. Right-click a client under Storage Pool; then, click **Set Priority**.
2. In the displayed window, select the wanted priority and click **OK**.

Claiming a repository
When a repository is claimed, the configuration of the FastBack Server changes.

The following scenarios provide examples of when you want to claim a repository:
- When the name of the FastBack Server changes.
- When the FastBack Server is corrupted and rebuilt.
- When you upgrade from the Tivoli Storage Manager FastBack Try and Buy to Tivoli Storage Manager FastBack Version 6.1.3 or later.
- When the FastBack Server moves to a new domain, you need to claim the repository again.

To claim a repository, complete the following steps:

1. Verify that no FastBack Server is using the repository. The claim repository option is disabled if any FastBack Server, even a defective server, is using the repository.
2. In FastBack Manager, from the Configuration tab, select **General Configuration** > **Storage Pool**.
3. Right click **Repository Pool**; then, click **Claim Repository**. If a repository has open files or an application that is running, you cannot claim the repository.
4. Specify the fully qualified path to the `Locations.ini` file for the repository.

   Tip: The `Locations.ini` file is a hidden system file. You must clear the hide protected system files option before you can select or view this file.
5. Click **OK**.

Note: The data deduplication server IP address is specified with the StorageNetIPAddress property in the `Locations.ini` configuration file. For example:

```
StorageNetIPAddress=9.148.229.203
```

When the IP address of the computer that is running the StorageNet server changes, the StorageNetIPAddress property in all `Locations.ini` configuration files must be manually updated with the new IP address.

Removing a folder, volume, or disk from the repository

Folders, volumes, or disks controlled by the connected FastBack Server can be removed from the repository.

To remove a disk from the repository, right-click the disk and click **Remove from repository (with snapshot relocation)**. For a repository not enabled for data deduplication, at least two repository disks must be present to use this option. For a repository enabled for data deduplication, only one repository disk can be used.

Selecting the **Remove from repository (with snapshot relocation)** option distributes the data if space is available. If there is not enough space to relocate the repository contents, the operation fails and the process stops. You can add more repository space for relocation, and initiate the process again.

No progress bar of removing the repository is displayed. The repository is removed in the background.

Setting up snapshot policies

Snapshot policies link client groups to a job schedule, specify the number of snapshots that is to be retained, and identify snapshot priority. A policy cannot apply to a FastBack Client that runs on both Windows and Linux. A policy applies to either a FastBack Client that runs on a computer that is using a supported Microsoft Windows operating system or a FastBack Client that runs on a computer that is using a supported Linux operating system.

Important: (Linux only) Before you set up a snapshot policy, for any hard disk that is backed up with Tivoli Storage Manager FastBack, ensure that the disk signature that is not 0. You can meet this prerequisite by using the FastBack Disk Signature utility. Reference the instructions in the "Software requirements and prerequisites" on page 33 section for more information.

Snapshots run according to the configured snapshot policies, where each snapshot policy requires two objects:

- Client groups
- Job schedules

You can create a snapshot policy by using one of the following procedures:

- Using a wizard to guide you through the required steps.
- Using the Configuration tab to create client groups and job schedules manually, and then to combine client groups and job schedules into a policy.

When you use Tivoli Storage Manager FastBack snapshot policies with Tivoli Storage Manager, use Unicode characters to name the snapshot policy, job schedule, and client group. However, the following Unicode characters are not supported:

: / , ; \ * ? " < > | ^ ' .

An error occurs when you use one of these characters. In addition, tab and newline are not allowed.

Tivoli Storage Manager FastBack does not support the use of the apostrophe when naming the snapshot policy, job schedule, and client group.

Snapshot policies that are created through a wizard can be managed and changed by using the Policies pane, from the Configuration tab.

After the policy is created, clients groups can be added, changed, or removed. The job schedule can be changed, but you cannot add a schedule or remove the existing schedule. When you change a snapshot policy, the changes are applied only after running jobs, cleanup, and erase chain procedures are completed.

If a policy is added while another snapshot is in progress, the snapshots for the new policy do not start until the snapshot that is in progress completes.

When you schedule and run snapshots, if the client has an EISA partition, create a snapshot of the volume with this EISA partition. IBM Tivoli Storage Manager FastBack for Bare Machine Recovery of EISA partitions must be included in the backup snapshot in order for the system to be properly restored.

Running defragmentation on volumes protected by Tivoli Storage Manager FastBack results in large incremental snapshots and might cause a failure.

For the supported Windows 2008 and Windows Vista operating systems, the defragmentation task runs automatically on all volumes. To disable the defragmentation task, open the Task Scheduler. You can open the Task Scheduler from the Windows Start menu. Click **Programs** > **Accessories** > **System Tools** > **Task Scheduler**. Navigate to **Task Scheduler (local)** > **Task Scheduler Library** > **Microsoft** > **Windows** > **defrag**. From this window, disable the ScheduledDefrag task.

Client groups

Client groups identify the volumes that are backed up. In addition to volumes, client groups can also back up SQL and Exchange databases. The SQL and Exchange databases that are backed up can span across multiple disk volumes.

Use the following scenario to help maintain client groups: A volume with signature *A* is mounted to a specific mount point, and a client group that is using this mount point is created. Next, the volume is unmounted, and a different volume with signature *B* is mounted to the same mount point. The FastBack Manager displays the following message:

```
FBSG5815I The volume configuration of the following FastBack
Client has changed <volume_info>. Super user should
delete and rebuild the affected client group if any.
```

Going into the affected client group, the volumes are displayed as they must be. For the new signature to be associated with the mount point, click **Apply**, otherwise the FastBack Manager and FastBack Server associate the old signature with the mount point.

Job schedules

Job schedules are used to set the following attributes:
- The time the snapshot is taken
- The type of snapshot that is taken

Using wizards to create snapshot policies

After disks are added to the repository, the snapshot policy can be set up using the snapshot policy wizards.

Note: SQL Server 2008 databases are not displayed in the snapshot policy wizards. To work around this issue, you can back up the entire volume that contains the SQL database.

There are three wizards to guide you through the steps required to create snapshot policies at different complexity levels:

Create Snapshot Now Wizard
> Use this wizard to create a single-instance snapshot of a user-defined group of volumes. The snapshot runs within 2 minutes unless the maximum number of simultaneous full or incremental delta block snapshots is reached.
>
> For the maximum number of simultaneous full and incremental delta block snapshots, the default value, *3*, is not to be changed.

Simple Policy Wizard
> Use this wizard to configure periodic snapshots of a user-defined group of volumes.

Advanced Policy Wizard
> Use this wizard to guide you through the configuration of client group, job schedule, and policy. When you use this wizard, you can use predefined job schedules and client groups.

Using the Create Snapshot Now wizard

Use this wizard to take a single, full snapshot of a selected set of volumes. You can take the snapshot immediately (within 2 minutes from the moment the command is activated), or at a preset selected time.

About this task

The created policy is displayed in the tree, under Policies. The job schedule and client group for the snapshot are also displayed under the corresponding categories in the tree. The job schedule and client group can be edited for additional use. For example, you might want to edit the schedule to create additional snapshots.

Procedure

1. Click the **Wizard** icon, .
2. Select **Create Snapshots Now**.
3. In the displayed window, select the volumes to back up. A client group name corresponding to the selected volumes is automatically assigned.
4. Select the start date and type a start time.
5. Enable or disable `Disaster Recovery` for this snapshot. If enabled, the snapshot is replicated by FastBack DR Hub Server.
6. Click **Apply**. The snapshot is taken according to the specified start time. The following three objects are created: client group, job schedule, and policy.

Using the Simple Policy Wizard

Use this option to configure snapshots that run periodically at user-defined intervals. You can also use this wizard to define a time of day when snapshots do not run. This exclusion period usually includes hours when workload is high.

Procedure

1. Click the **Wizard** icon, .
2. Click **Simple Policy Wizard**.
3. Select the volumes to back up. A client group name corresponding to the selected volume is automatically assigned.
4. Select and complete parameters.
5. Enable or disable Disaster Recovery for this snapshot. If enabled, the snapshot is replicated by the Disaster Recovery procedure.
6. When you are finished, click **Apply** to save the configuration. The snapshots are scheduled at the set times.

What to do next

You can define daily periods of time when the snapshot does not run. Excluding daily periods of time is useful for adjusting your bandwidth load and server workload during busy hours. To identify times to exclude, select **Exclusion Period**. Enter time values to exclude.

Using the Advanced Policy Wizard

The Advanced Policy Wizard guides you through the process of creating snapshots. The wizard provides most of the configuration options that are available when the policy elements are defined separately. To use the wizards to create snapshots and to create new schedules, policies, client groups, users, and user groups, you must have administrator permissions.

Before you begin

The procedure consists of the following steps:
1. Select or create the client groups for the policy.
2. Select or create the schedules for the policy.
3. Assign the policy parameters.

The job schedule for the policy and client group elements, created by the Advanced Policy Wizard, can be viewed and edited through the Browser pane.

In addition, you can define daily periods of time when the snapshot does not run. Excluding daily periods of time is useful for adjusting your bandwidth load and server workload during busy hours. In the **Job Schedule** pane, activate the **Exclusion Period** field and enter the From and To time values by using the 24–hour clock definition (where 12:00 is noon and 24:00 is midnight).

About this task

To create a snapshot policy through the Advanced Policy Wizard, complete the following steps:

Procedure

1. From FastBack Manager, click the **Scheduling Wizard** icon, .
2. Click **Advanced Policy Wizard**.
3. The first step in the wizard requires that you specify a client group. You can either create a client group or use an existing client group. Use one of the following procedures:
   - To define a new client group, complete the following steps:
     a. Select the Define a New Client Group tab.
     b. Type a client group name.
     c. Select volumes to assign to this client group.
     d. Click **Add**.
     You can create more than one client group for the policy.
   - To use an existing client group, complete the following steps:
     a. Select the Use an Existing Client Group tab. A list of client groups is displayed.
     b. Select client groups from the list.
     c. Click **Next**.
4. The Job Schedule window is displayed. You can either create a job schedule or use an existing job schedule. Use one of the following procedures:
   - To define a new job schedule, complete the following steps:
     a. Select the Define a New Job Schedule tab.
     b. Type a job schedule name.
     c. Select a type:

        Full forever
                All snapshots are full snapshots.

> **Incremental forever**
>> The first snapshot is a full snapshot. All subsequent snapshots are incremental snapshots.

    d. (Windows only) Decide whether to enable Continuous Data Protection (CDP). To enable CDP, select the check box.For more information about CDP, see "Continuous Data Protection (Windows only)" on page 141.

    e. In the Run every section, specify how often the snapshot is to run. If you want to run the snapshot daily, type a time under **Run once a day at**. The time you type is the time when the snapshot is run.

       For the **Run every** section, to prevent the job from running during specific periods of the day, enable and define the **Exclusion Period**.

    f. In the `Perform task on` section, select the days that the policy is to run.

    g. Click **Next** to save the new job schedule.

- To use an existing job schedule, complete the following steps:

    a. Select the Use an Existing Job Schedule tab. A list of job schedules is displayed.

    b. Select a job schedule from the list. Click **Add**.

    c. Click **Next**.

5. A summary window is displayed. The window provides an overview of the job schedules and client groups currently assigned to this policy. The window also includes other options and parameters that you can set for this policy. You can use this window to change the policy setup before you save it. The following list details the additional options and parameters:

Enable DR
> Enable or disable the Disaster Recovery function for this snapshot. If enabled, the snapshot is replicated by the Disaster Recovery procedure.

Number of generations
> Determine the number of snapshot generations that are retained. Older snapshots are cleaned up.

> **Tip:** Set the number of generations to exceed the actual number that are retained. If the number of generations is set too low, snapshots that exceed the generation value are placed in the cleanup queue during the restore operation. As a result, you cannot view that the restoring task is still running in the Snapshot Monitor.

Snapshot priority
> Set up the snapshot priority. If several snapshots are running at the same time and exceed the system resources, the snapshots are taken or discarded according to their preset priority.

You can change the list of assigned client groups according to the following rules.

- To add a client group, click **Add**. Select a client group. Click **OK**.
- To delete a client group, select the group and click **Remove**.
- To edit a client group, select a client group and click **Go To** in the corresponding pane.

Job schedules cannot be added or deleted.

6. Click **Finish**. The policy is added to the list of policies. The policy runs according to the job schedule.

Results

After you create the policy, you can run an immediate backup using the policy. To complete this task, in FastBack Manager, on the **Configuration** tab, under the **Policies** entry, locate the policy you created. Right click to select the policy; then, click **Perform Incremental Snapshot**.

Pre or Post Processes

The Pre or Post Processes tab allows you to customize the backup process by adding various scripts to the snapshot policy.

Snapshots run according to a policy. As a part of the policy, you can specify pre and post processes. These processes are scripts that run when the snapshot is created. Pre and post processes run on a FastBack Client. You can specify a timeout parameter that cancels the script if it does not complete with a predefined time period. In addition to canceling the script, the snapshot is also canceled.

There are sample scripts that are available in the FastBack Client directory:
`C:\Program Files\Tivoli\TSM\FastBack\client\scripts`

In addition, there is information that describes how to use these sample scripts for specific database applications in Chapter 11, "Best practices," on page 233.

The Pre or Post Processes can be specified when creating a policy with the Advanced Policy wizard. In addition, you can specify Pre or Post Processes when manually editing a policy.

To add a script to the policy by using the Pre or Post Processes tab, complete the following steps:

1. Select the types of scripts you want to include. There are three types of scripts you can include:
   - **Pre consistency-point**: The script runs before a consistency point when the application flushes all buffers to the disk.
   - **Pre Snapshot**: The script runs after a consistency point when the application flushes all buffers to the disk, and before the snapshot.
   - **Post Snapshot**: The script runs after a snapshot is complete. This script can be used for activities that restore the system to the status that existed before running the snapshot.
2. For the types of scripts you choose to include, verify that the script is stored on the system.
3. Type the script name that you want to run.
4. Specify a time, in minutes, for **Cancel process if it is not completed within**. The default value is *10* minutes. The minimum timeout value is *1* minute. The maximum timeout value is *1200* minutes (20 hours).

   If the script does not complete in the amount of time allocated, the script is canceled. Twenty minutes after the script is canceled, the snapshot terminates. If the snapshot is complete before the script completes, the status is displayed as successful.

Policy cleanup
About this task

Use the **Policy Cleanup** tab to override the default cleanup definition and set a unique cleanup level for the selected policy.

Note: The default definition is set through **General Configuration** > **Maintenance** > **Cleanup**. For more information about policy cleanup, see "Cleanup configuration" on page 178.

Procedure

1. Click **Restore default**.
2. Set the cleanup level for the policy by selecting one of the options.
3. Click **Apply**.

Verifying pending jobs

Pending jobs can be verified by clicking the Pending jobs category in the menu tree.

Creating snapshot policies manually

Each policy comprises one or more selected client groups and one job schedule. These client groups and job schedule are created either automatically through one of the wizards or individually.

Regardless of how the policies are created, client groups and job schedules are listed under the corresponding category in the tree. The client group and job schedule pools can be used as a source for creating the policy manually. This section describes how to manually create client groups and a job schedule pool, and how to create various policies based on selected elements from the pools.

Creating client groups

You can create more than one client group for the policy.

Before you begin

Note: Clients can only be added to client groups using their host name, and not the IP address.

About this task

To create a client group, complete the following steps:

Procedure

1. From FastBack Manager, right-click **Client groups**, and then click **New client group**.
2. Type a client group name.
3. Select volumes to assign to this client group. Click **Add**. If you are backing up data from a Microsoft SQL database or a Microsoft Exchange database, the services for the SQL and Exchange databases are to run on the FastBack Client system. For example, if you want to back up SQL data, *volume D:* can store the database and *volume E:* can store the logs. Ensure that service is started so you can select the SQL databases as a part of the client group selection.
4. Click **Apply**. The client group is to be displayed under the **Client groups** node in the tree.

Results

When you schedule and run snapshots, if the client has an EISA partition, create a snapshot of the volume with this EISA partition. IBM Tivoli Storage Manager

FastBack for Bare Machine Recovery of EISA partitions must be included in the backup snapshot in order for the system to be properly restored.

To remove a client group, right-click the group and click **Remove**.

Creating a job schedule
About this task

To create a job schedule, complete the following steps:

Procedure
1. In the Configuration tab, right-click **Job Schedules** and select **New Job Schedule**.
2. Type the job schedule name. By default, a sequentially numbered job schedule name is assigned.
3. Select a job type:

   Full forever
   > All snapshots are full snapshots.

   Incremental forever
   > The first snapshot is a full snapshot. All subsequent snapshots are incremental snapshots.
4. (Windows client only) Decide whether to enable Continuous Data Protection (CDP). To enable CDP, select the check box. If the repository is a data deduplication repository, CDP is not available. For more information about CDP, see "Continuous Data Protection (Windows only)" on page 141.
5. In the **Run every** section, specify how often the snapshot is to run. If you want to run the snapshot daily, type a time under **Run once a day at**. The time you type is the time when the snapshot is run. For the **Run every** section, to prevent the job from running during specific periods of the day, enable, and define the **Exclusion Period**.
6. In the `Perform task on` section, select the days that the policy is to run.
7. (Optional) (Windows only) You can click **Application Aware** to change the following parameters:

   Preserve application consistency
   > Creates consistent database snapshots by using quiescing. There are two quiescing options: either the Volume Shadow Copy service or IBM application quiescing.

   > You cannot use application quiescing and the VSS service at the same time. In addition, you cannot use VSS application quiescing to back up utility partitions.

   > Use IBM application quiescing for supported Windows 2000 and Windows XP operating systems.

   > Use VSS application quiescing for supported Windows 2003 and later operating systems. If you need an application-aware snapshot, do not use VSS application quiescing.

   > To back up applications that run on supported Microsoft SQL and Microsoft Exchange servers, verify that the VSS service is supported to take snapshots of the application.

Purge Exchange server log files
> Deletes Exchange logs that are already committed to the database before the snapshot.

8. (Optional) To specify additional parameters, click **Advanced**. The following list describes the parameters that you can change. When you finish work in this window, click **OK**.

   - Initial time: You can change the default time.
   - To stop running the job on a specific date or after a specific number of snapshots are taken, select **Short range job**.
   - To identify and back up only the used areas of NTFS volumes during full and incremental snapshots, select **Content aware snapshot**.

   Note: In the user interface that you use, the format for the time field might not exactly match the figure in this section. The time format varies depending on the regional settings for your system.
9. To create the job schedule, click **Apply**.

Managing snapshot policies

Policies can be created by using either wizards, or manually by creating the separate elements that consist of client groups, job schedules, and policies. Whether the policies are created by using wizards or manually, the policy elements are listed in the appropriate category in the tree under client groups, job schedules, and policies. These objects can be changed at any time through the appropriate configuration tree option.

About this task

To edit a policy, complete the following steps:

Procedure

1. Select a policy under Policies in the categories tree.
2. Change parameters as wanted. The **Enable DR** option cannot be changed after the policy is created.
3. To delete a client group, select a client group and click **Remove**.
4. To open a client group, click **Go to**.
5. To add a client group, click **Add**, select the wanted element, and click **OK**.
6. Click **Apply** to apply the changes.

What to do next

If you remove a policy from FastBack Server, all the snapshots that are related to that policy are also deleted from the repository. During that time, there is no scheduling of new snapshots.

To delete a policy, right-click a policy; then, click **Remove**. You are prompted to remove the corresponding job schedules and client groups that are not connected to any other policy.

Primary storage layout changes

When changes to labels or volumes are made in any of the FastBack Client servers, the changes are automatically identified by the FastBack Server. FastBack Manager is updated accordingly. The corresponding client groups are not automatically updated.

The following rules apply when changing the primary storage layout:

- If a storage layout is changed, for example, if a volume is removed or resized, expanded or retracted, the corresponding client group must be updated manually. After volume deletion, the volume is displayed as an obsolete volume in the client group and the corresponding check box is not selected. For policies that are backed up, the deleted volume fails. Click **Apply** in each client group that contains the deleted volume. This action updates the client group and policies with the change.
- Changing the drive letters on protected servers brings up a dialog in FastBack Manager that prompts you to review the relevant client groups.
- Deleting volumes or partitions while the corresponding snapshot is in progress causes the snapshot to be stopped.

Changing the global application-aware parameters (Windows only)

The global default settings for application-aware backups are set in the application tab. Some of these settings can also be set while configuring new policies.

About this task

To change the global application-aware parameters, complete the following steps:

Procedure

1. Click the **Configuration** > **General Configuration** category and select **Applications**.

   Preserve application consistency
   > Creates consistent database snapshots by using quiescing. There are two quiescing options: either the Volume Shadow Copy service or IBM application quiescing.

   > You cannot use application quiescing and the VSS service at the same time. In addition, you cannot use VSS application quiescing to back up utility partitions.

   > Use IBM application quiescing for supported Windows 2000 and Windows XP operating systems.

   > Use VSS application quiescing for supported Windows 2003 and later operating systems. If you need an application-aware snapshot, do not use VSS application quiescing.

   > To back up applications that run on supported Microsoft SQL and Microsoft Exchange servers, verify that the VSS service is supported to take snapshots of the application.

   Purge Exchange Logs after completed snapshot
   > Deletes Exchange logs that are already committed to the database before the snapshot. Available in non-VSS environments only.

   Application quiescing timeout (in minutes)
   > The maximum downtime for the Exchange Server Service while running a quiescent job. Available in non-VSS environments only.

   Job Schedule activity timeout (in minutes)
   > The maximum hang time for an in-progress snapshot. Change the application quiescing and the job scheduler activity timeouts at the request of support only.

2. For consistent data backup, enable application quiescing as follows:
   - For Microsoft Exchange 2007 or Exchange 2010, enable VSS application quiescing. The Exchange log files will be deleted automatically from the storage group after the snapshot completed successfully.
   - For Microsoft Exchange 2003, enable either IBM application quiescing or the VSS application quiescing. If you enable VSS quiescing, Exchange log files are deleted automatically from the storage group after the snapshot is completed successfully. If you enable IBM quiescing, then you need to ensure that **Purge Exchange Logs after completed snapshot** is enabled.
   - For Microsoft Exchange 2000, enable IBM application quiescing and ensure that the Exchange log files will be deleted automatically from the storage group by confirming that **Purge Exchange Logs after completed snapshot** is enabled.
3. Click **Apply** to save changes. All Exchange-related snapshot policies created from this point forward would be configured by default according to the new settings.

Configuring Volume Shadow Copy service (Windows only)

The Volume Shadow Copy (VSS) service, referred to as VSS application quiescing on the Tivoli Storage Manager FastBack user interface, is available for supported Microsoft Windows Server 2003 and later operating systems, including Windows Vista and Windows 2008. Do not use the VSS service to back up systems that run Microsoft Windows 2000 or Microsoft Windows XP.

Before you begin

Restriction: The hotfix associated with Microsoft Knowledge Base article 970770 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770) is required when backing up the domain controller on Microsoft Windows 2008.

When using Microsoft Windows Server 2003 SP2 (or later), make sure the hotfix associated with Microsoft Knowledge Base article 969219 (http://support.microsoft.com/kb/969219) is installed.

About this task

VSS creates consistent, point-in-time copies of data known as shadow copies. Do not use IBM application quiescing and the VSS application quiescing simultaneously. If you want an application-aware snapshot, do not use VSS application quiescing.

When you use the VSS service to take snapshots of servers, verify that the VSS service is supported by the applications that run on the servers. If the applications do not support VSS, the consistency of the application will not be ensured by the VSS service.

Tivoli Storage Manager FastBack implements a VSS software provider that creates snapshots, and ensures snapshot consistency and integrity. The following figure describes how the VSS interfaces with various components to create a shadow copy of a volume.
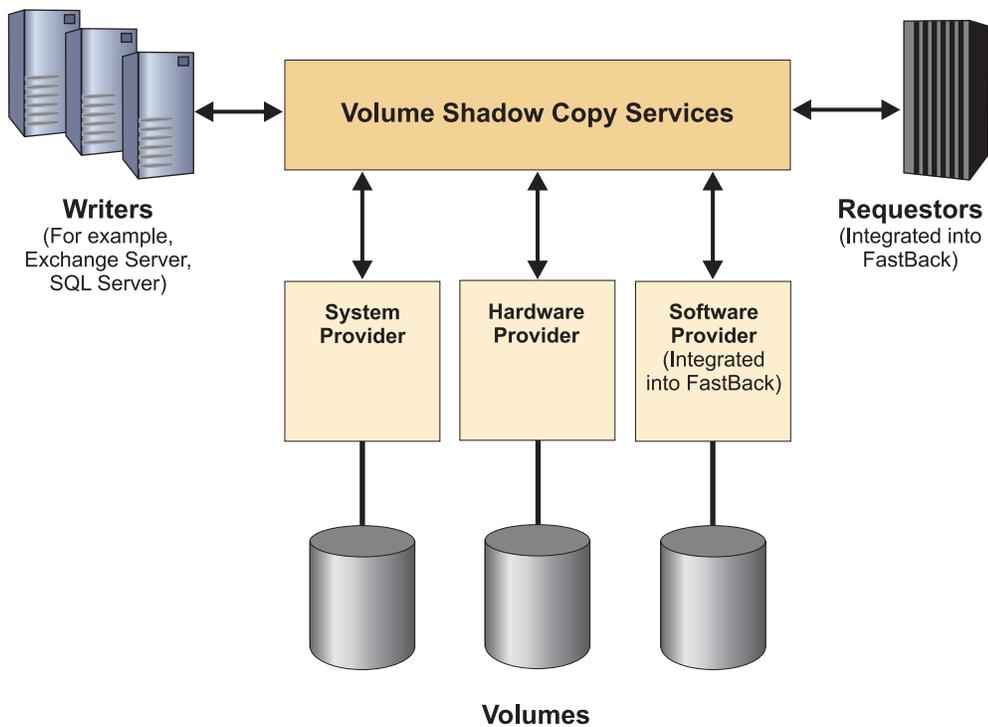
Figure 7. Volume Shadow Copy service architecture diagram

When you use FastBack Manager, by default, the VSS service enabled. The VSS service signals the writer applications to stop operation and to start a backup.

To disable the VSS service, complete the following steps in the General Configuration window:

1. From General Configuration, select the **Applications** tab.
2. Clear the **Preserve application consistency** selection.
3. Click **Apply**.

To enable IBM application quiescing, complete the following steps:

1. From General Configuration, select the **Applications** tab.
2. Select **Preserve application consistency** > **Use IBM application quiescing**.
3. Click **Apply**.

The VSS service can also be disabled for particular job schedules using the Job Schedule window:

Procedure

1. Select a Job Schedule.
2. In the Job Schedule window, click **Application Aware**.
3. Clear the **Preserve application consistency** selection.
4. Click **OK** > **Apply**.

What to do next

To enable IBM application quiescing from the Job Schedule window, complete the following steps:

1. Select a Job Schedule.
2. In the Job Schedule window, click **Application Aware**.
3. Select **Preserve application consistency** > **Use IBM application quiescing**.
4. Click **OK** > **Apply**.

Manual snapshot back up

You want to back up a snapshot manually before running server maintenance procedures or if you think a repository is corrupt.

There are three ways you can manually back up a snapshot:
- Take an incremental snapshot to manually add an incremental snapshot at the end of snapshots.
- Take a checkpoint snapshot to create an incremental delta block snapshot at the end of the snapshots chain, according to the policy configuration. This incremental delta block snapshot contains all changes from the last known good incremental delta block.
- Take a full snapshot of the policy volumes. This type of snapshot consumes a lot more system resources, in particular disk space.

These repair functions can be applied to either a single chain or all snapshot chains for a policy. The outcome of using one of the functions is a new incremental or full snapshot at the end of the snapshot chain. This ensures the existence of a reliable, recent data backup for the volumes of the policy to which it is applied.

Manually backing up a snapshot affects all the snapshot chains of the policy. For example, a checkpoint snapshot can be run on an Exchange database that is spread over several volumes.

To manually back up a snapshot, complete the following steps:
1. From FastBack Manager, go to the **Configuration Tab**.
2. In the navigation tree, locate the policies.
3. Right click to select a policy; then, click either **Run Incremental Snapshot**, **Run Check Point**, or **Run Full Snapshot**.

If you run defragmentation on volumes protected by Tivoli Storage Manager FastBack, a large incremental snapshot is created.

For the supported Windows 2008 and Windows Vista operating systems, the defragmentation task runs automatically on all volumes. To disable the defragmentation task, open the Task Scheduler. You can open the Task Scheduler from the Windows Start menu. Click **Programs** > **Accessories** > **System Tools** > **Task Scheduler**. Navigate to **Task Scheduler (local)** > **Task Scheduler Library** > **Microsoft** > **Windows** > **defrag**. From this window, disable the ScheduledDefrag task.

Mounting snapshots

FastBack Mount must be installed and operated from a system that can see the repository either through SAN or LAN. You can use FastBack Mount to mount any snapshot and use the snapshot to complete data recovery. FastBack Mount can operate in two modes: GUI and command line interface.

FastBack Mount on Linux

FastBack Mount can be installed and operated from any Red Hat Enterprise Linux 5.4 Server or SuSE Linux Enterprise Server 10 system. FastBack Mount on Linux systems provides the following features:

* Browse a list of snapshots available for restore.
* Create a virtual mount of a snapshot for a file-level restore or tape integration.
* Dismount the virtual mount volume after completing a file-level restore.
* Initiate an instant restore of a snapshot by providing a target mount point.
* Since a volume dismount is not required after the instant restore completes, the restored volume remains accessible.

Instructions regarding how to use FastBack Mount on Linux are available at "File-level restore and instant restore (Linux)" on page 134

FastBack Mount on Windows

FastBack Mount can be installed and operated from any Windows 2000 (or later) system. You can use FastBack Mount to mount any snapshot and use the snapshot to complete data recovery.

For systems that run Windows Vista or Windows 2008, FastBack Mount can run in the following two modes:

* When no users are logged in, FastBack Mount runs as a service. The FastBack Mount service enables remote connections through the Administrative Command Line.
* When a user is logged in, FastBack Mount continues to run as a service until you start the FastBack Mount application and use the FastBack Mount graphical user interface. When you close the FastBack Mount application and graphical user interface, the FastBack Mount service restarts.

  To start FastBack Mount, from the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Mount**.

  You can use only the FastBack Mount application and graphical user interface when running with administrator login credentials. Only one copy of the FastBack Mount application can be active at any time.

For Windows 2008 systems, because FastBack Mount, like all FastBack services, is installed as a local system account, when you try to configure FastBack Mount access with this setting, the **Domain** list might have no entries displayed. (The **Domain** list is part of FastBack Manager. In the navigation tree, select **General Configuration**. In the main window, select **FastBack Mount Access**. The **Domain** list is on this page.)

When there are no entries in the **Domain** list, FastBack Mount cannot access snapshots. This problem can be resolved by going to the Services window and changing the Log On properties. Specifically, change **Local System account** to **This account**. For **This account**, specify a domain administrator ID and password. Click **OK** to save the changes. Restart the FastBack Server service. The **Domain** list displays entries.

If you want to restore files on a computer that runs a supported Linux operating system, you can use FastBack Mount. From the computer that runs a supported Windows operating system and FastBack Mount, start FastBack Mount. When you select a mount destination, select mount as an iSCSI target. From the Linux system,

you start the iSCSI initiator and login to the Windows system that runs FastBack Mount. You can then create a local mount directory and mount the new device to the local directory. When you finish the file recovery task, you can unmount the target. For more detailed instructions, go to "Recovering files" on page 127

FastBack Mount saves changes to data on a virtual volume in the write cache. The write cache is enabled by default, the path is `C:\Documents and Settings\All Users\Application Data\Tivoli\tsm\FastBack\mount` and the size is set to a maximum of 90% of the available space. These settings can be configured by clicking the settings in the main FastBack Mount window, or by editing the configuration file `FastBackMount.conf`. The write cache must be on a local drive and cannot be set to a path on a shared folder. If the write cache is disabled, changes to the data on a virtual volume is stored in RAM.

The FastBack Server does not have to be running when you use FastBack Mount.

FastBack Mount security (Windows only)

Security restrictions for mounting virtual volumes depend on the type of repository.

Local/SAN repository
> Non-administrator Active Directory users can mount only snapshots of volumes when they have the correct share access privileges defined. Non-administrator *Xpress-Restore* domain users can mount volumes on servers they have access to, according to the permissions set by the Tivoli Storage Manager FastBack user management mechanism. Administrators can mount any volume. Click **Login as** to change the user ID you use to log on.

Share repository
> Any user that has access to the share can mount any snapshot.

After the volume is mounted, NTFS security is applied automatically by Windows operating systems based on the current user's account, regardless of the account that was used to mount the volume.

Using FastBack Mount and Veritas NetBackup (Windows only)

Veritas NetBackup version 5.1 and later is supported.

Before you begin

Previous knowledge of Veritas NetBackup and Tivoli Storage Manager FastBack is required.

Note: Back up to tape is faster when a full cleanup is carried out before the backup is run.

About this task

To configure Veritas NetBackup for use with FastBack Mount, complete the following steps:

Procedure

1. Install the NetBackup server and clients on different systems. For NetBackup server and client installation instructions, see the Veritas NetBackup product

documentation. When installing the NetBackup server and clients for use with FastBack Mount you must also meet the following prerequisites:

- The NetBackup client must be installed on a system with Windows XP Service Pack 1 or later.
- FastBack Mount and Administrative Command Line must be installed on the same system as the NetBackup client. Do not install firewall, anti-virus, or anti-spyware software on this system. When anti-virus and anti-spyware applications run simultaneously with FastBack Mount, there is high processor usage, resulting in snapshots that run slowly or are stopped. In rare cases, running FastBack Mount with anti-virus and anti-spyware applications can also cause a Windows system crash. If a system crash occurs, reboot the system. The system will start normally.

  During FastBack Mount and Administrative Command Line installation, when asked for IP address, type the IP address for the NetBackup client. Alternatively, if FastBack Mount is already installed, open the `FastBackShell.ini`, and manually configure the IP address for the NetBackup client. The file `FastBackShell.ini` is in the following path `C:\ProgramFiles\Tivoli\TSM\FastBack\shell`.

2. Run full backups.
3. Verify that the NetBackup client is configured to *0* retries.
4. For the Active Directory user that is logged on to the NetBackup client, give NTFS permissions to the volumes. These volumes are backed up by the NetBackup software.
5. For every NetBackup policy, back up a single volume.
6. Increase the **Client Read Timeout** parameter to *900 seconds*.

What to do next

To create a backup, complete the following steps:

1. To receive information about volumes available for tape backup, on the NetBackup client system, run the following command:

```
FastBackShell -c mount dump -type share -rep P -for TapeBackup -reparse
 P [-file P]
```

   For more information about the parameters, use the following list:

   -rep   Use this parameter to specify the FastBack Server repository. Use the network share followed by user name and password with permissions to see the repositories. For example,

   share: \\hostname\share user=username pass=password

   -reparse

   Use this parameter to specify the volume name for automatic reparse points. The default is *C:*.

   -file   Use this parameter to specify the file name for the dump file. For example,

   `C:\tape\dump_con_share.txt`

   For an example of this command with parameters, see the following code sample:

```
"%dir%FastBackShell.exe" -c mount dump -type share -rep "share:
 \\computer_name\folder_path\London-FastBack\repository user=tapeadmin pass=
 admin123 domain=Taurus" -for TapeBackup -reparse c: -file C:\tape\
 dump_con_share.txt
```

The resulting dump file, for example, `C:\tape\dump_con_share.txt`, looks like the following sample:

```
 "%dir%FastBackShell.exe" -c mount add -ro -rep
"share: \\Con\ London-IBM\repository user=tapeadmin
pass=admin123 domain=Taurus" -target "c:\Con(092)London-IBM
(092) repository(092)\Policy-DC\London-DC\C\\" -policy
"Policy-DC" -server "London-DC" -volume "C:\\" -date "last
snapshot"
```

(092) stands for backslash in the part of the target path that represents the location of the repository. If there are multiple volumes in a repository, separate lines are created for each volume.

2. Create a new batch file in a directory on the NetBackup client system. For example, create the `mount.bat` file. You can use the following code samples to help complete this step:

```
set dir=c:\Program Files\Tivoli\TSM\FastBack\shell\
 ...

 IF %ERRORLEVEL% EQU 0 goto end

 :error_end

 echo could not mount

 EXIT 1

 :end

 EXIT /B 0
```

When using this sample, use the following guidelines:
- *dir* must specify the full path to the `FastBackShell.exe` file.
- Paste the contents of the dump file into `mount.bat` instead of the *...* line.
- Replace *C:\Con(092)London-IBM (092)repository(092)* with the folder that you want the volume to be mounted to. For example, `C:\mount`.
- If the dump file has more than one command, use only one command with the volume that you want to back up in this particular policy.

3. Run the following command to mount the latest snapshot to a mount point: `mount.bat`. For a sample mount point, see the following example:

```
c:\ mount\Policy-DC\London-DC\C
```

4. Open the NetBackup Administration Console and create a policy. To create a policy, you can complete the following steps. In these steps, the new policy wizard is not used, but you can use the wizard.

   a. In the Add New Policy window, go to **Attributes** and click **Cross Mount Points**.

   b. Choose a predefined destination. For the policy type, select *MS-Windows-NT*.

   c. Go to the Schedules tab to create a schedule.

   d. Go to the Clients tab to select the NetBackup client system.

   e. Go to the Backup Selections tab to type the full path to the mount point. For example, `D:\Orion\rep\Policy-G\Apollo-Exchange\G`

5. On the NetBackup client, in the `bin` directory, a `bpstart_notify.Tape_Backup.bat` file must be created. For additional policies, substitute the name of the policy instead of *Tape_Backup* in the file name. The `bpstart_notify.***.bat` file needs run before the backup. If the backup fails,

the backup is stopped. To mount the snapshot before back up starts, call
mount.bat. The following example demonstrates how to call mount.bat:

```
call c:\Tape\mount.bat >> c:\tape\pre.log 2>&1
echo %errorlevel% > %6
```

If the volume is not mounted, the next backup might fail.

6. On the NetBackup client, in the bin directory, a bpend_notify.Tape_Backup.bat
   file must also be created. The Bpend_notify.***.bat file is run after the backup
   finishes.

7. On the NetBackup client system, create a new batch file, for example,
   dismount.bat, in the following directory on the NetBackup client system:
   C:\Tape. For an example of how to unmount the snapshot after the backup is
   finished, see the following code sample:

```
call c:\Tape\dismount.bat >> c:\tape\pst.log 2>&1
echo %errorlevel% > %6
```

Run the dismount.bat file to unmount the previously mounted snapshot.

8. On the NetBackup client system, create a new batch file in a directory. For
   example, create the start_backup.bat file in the C:\Tape. You can use the
   following code samples to help complete this step:

```
@ECHO OFF

bpbackup -i -p Tape_Backup -s diff_incr
REM Checking group was not started
if %ERRORLEVEL% == 0 goto END
echo Backup was not started
:END
```

9. To back up to tape, run start_backup.bat.

Volume and file recovery

With the snapshots that are stored on the FastBack Server, you can recover data
that is backed up. The following sections describe how to recover files and
volumes, including how to complete an instant restore of volumes.

Volume recovery

Volume restore restores an image of the original volume. Volume restore and
instant restore can restore an image only to a basic disk or to a simple volume, and
not to dynamic disks.

Volume restore restores an image of the original volume. Volume restore and
instant restore can restore an image only to a basic disk or to a simple volume, and
not to dynamic disks.

When you complete a **Disk Restore**, if open, close the disk management utility
that is a part of Windows system management tools. Volume-level restore
operations are done from the Snapshots Monitor pane or from the Recovery pane,
by choosing the specific snapshot to be restored.

Before doing a volume restore, review the following list of possible limitations:

- Volume restore cannot be done in the following cases:
  - The destination volume includes an operating system or page file.
  - The destination volume is part of software RAID.

- The snapshot is running on the target volume, or on any volume that belongs to the same policy.
- Volume restore fails if there are open files or an application that is running on the destination volume. You can force a restore on a destination volume that has open files or applications by selecting **Ignore open handles on the destination volume**. Ignoring open files and applications on the destination volume can cause a problem with applications, including the loss of data in files that are open on the target volume.
- If the FastBack Server does not respond during volume restore, or the volume restore is stopped, the restored volume stays unmounted, and its data is invalid. In this case, either remove or format the volume. Alternatively, if another restore attempt was successfully completed, the volume must be mounted again.

File recovery

Administrators can use FastBack Mount for efficient file-level recovery and to minimize downtime by mounting snapshots to virtual volumes.

The virtual volume can be viewed with any file manager, for example Windows Explorer. The directories and files in the snapshot can be viewed and managed like any other file. If you edit the files and save your changes, after you unmount the volume, your changes are lost because the changed data is held in memory and never saved to disk. Because the changes are written to memory, FastBack Mount can use a large amount of RAM when working in read/write mode.

You can copy the changed files to another volume before unmounting. On Microsoft Windows XP and Microsoft Windows 2003 operating systems, you can select *read only* as a mounting option. For Windows 2000 servers, the *read only* option is not supported.

FastBack Mount can mount snapshots from more than one source:
- Local or SAN repository
- Shared repositories on the network, either after replication or attached to FastBack Server

FastBack Mount can be used for the following tasks:
- Speeding up archiving to tape and other media
- Efficient copying of large amount of data on the SAN
- Mounting database applications for batch reports
- Quickly verifying snapshots and the database

File-level recovery is not supported for FastBack Server repository data on Tivoli Storage Manager tape media. If you want to use FastBack Mount for file-level recovery of data that is stored on tape, the data needs to be moved to disk or file storage. This can be done in Tivoli Storage Manager by using the `QUERY OCCUPANCY` command to see where the data is stored, and then by using the `MOVE NODEDATA` command to move this data back to disk or file storage. For more information about these commands, see the Tivoli Storage Manager Information Center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2/index.jsp

Instant restore

You can use instant restore to start accessing data on the same disk where the volume is being restored, while the restore operation is in progress.

Instant restore works only with mounted volumes. Mounted volumes must have an assigned drive letter.

You can complete an instant restore of a volume in a supported clustered environment. While instant restore process is running, you can access the volume. Other volumes in the cluster are not affected and you can work with the cluster, and with that volume, in parallel. During the instant restore the disk that is being restored cannot fail over, in the event the node fails.

If a system is shut down while instant restore is in progress, the instant restore automatically continues from the same point when power is restored.

Instant restore destination volumes must be either on basic disks, or simple volumes on dynamic disks. Destination volumes cannot be spanned volumes, mirrored volumes, or RAID-5 volumes. You can use a basic disk as a destination volume and then convert the basic disk to a dynamic disk.

Instant restore is not supported for FastBack Server repository data on Tivoli Storage Manager tape media. If you want to use instant restore to restore data that is stored on tape, the data needs to be moved to disk or file storage. This can be done in Tivoli Storage Manager by using the **QUERY OCCUPANCY** command to see where the data is stored, and then using the **MOVE NODEDATA** command to move this data back to disk or file storage. For more information about these commands, see the Tivoli Storage Manager Information Center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2/index.jsp

Restoring volumes

You can restore a volume to a selected destination where all of the volume data can be accessed.

Before you begin

Before you start restoring a volume, complete the following steps:
1. From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Manager**.
2. In the logon window, type your user name. The default user name is *admin*.
3. Type your password. The default password is *admin123*.
4. Select a domain. The default domain is *XPRESS-RESTORE*. After you select the domain, the configuration is loaded. This process might take a few minutes. You cannot click Login until the configuration is loaded.
5. Click **Login**.
6. Verify that the Microsoft Windows share representing the FastBack Server repository is available. The client is to point to the share for the restore process to be successful. To complete this step, use the following procedure:
   a. From the Windows Start menu, select **Control Panel**.
   b. Open Administrative Tools.
   c. Open Computer Management.
   d. In the navigation tree, expand **Shared Folders**. To go to the default shared folder without knowing the name of the repository disk or repository folder, type the following string and you can connect to the FastBack Server shared repository: \\ServerName\rep

About this task

When you run a volume restore, you restore an image of the original volume. To restore a volume, complete the following steps:

Procedure

1. In FastBack Manager, from the **Snapshots Monitor** tab, right-click the snapshot to be restored; then, click **Restore** > **Snapshot Volume Restore**. When you select the snapshot, ensure that the policy and snapshot correspond to the FastBack Client system.
2. Select the destination volume where you want the volume restored. Verify that the size of the target is equal to, or greater than the size of the volume to be restored. Otherwise, the restore process does not complete.

   Attention:
   - Restoring a volume to a viewable storage volume involves overwriting data on that existing storage volume. After the restore begins, the current volume contents are permanently erased. Before you start the restore, verify that the correct volume is selected, and that there are no open handles or processes that use that volume.
   - The restore operation fails if there are open files or applications that are running on the target restore volume. On a FastBack Client running with the Microsoft Windows operating system, select **Ignore open handles on the destination volume**. This selection causes Tivoli Storage Manager FastBack to ignore the open files and applications that are running on the destination volume. This situation can cause a problem with applications and loss of data in files that are open on the target volume.

     If the FastBack Client is running on a computer with the Linux operating system and you select **Ignore open handles on the destination volume**, the selection is ignored. You must manually stop all open files and processes on the Linux client volume where you want to restore before running a volume recovery.

3. Click **Apply**. In response to the verification message, click **Yes**.

   Note: After the restore process is complete, the target volume is not displayed from the FastBack Manager. The target volume is not displayed because the volume is not mounted.

4. (Linux only) After the volume restore is complete, manually mount the volume with one of the following commands:
   - If the mount point is permanent, use the following command:

     ```
     mount -a
     ```
   - If the mount point is temporary, use the following command to specify the device and directory:

     ```
     mount <device_name> <directory>
     ```

   Remember: Root credentials are required to run `mount` commands.

Recovering files

About this task

Administrators can use FastBack Mount for efficient file-level recovery and to minimize downtime by mounting snapshots to virtual volumes. On supported Windows operating systems, file-level recovery is supported on NTFS volumes.

Note: File-level recovery is not supported for FastBack Server repository data on Tivoli Storage Manager tape media. For more information, see "Volume and file recovery" on page 124.

(Linux only) To run a file-level recovery for a Linux system, see "File-level restore and instant restore (Linux)" on page 134.

(Windows only) To run a file-level recovery for a Windows system, complete the following steps:

1. Use administrator credentials to log on to the FastBack Client system where you want to restore files. FastBack Mount is installed on the FastBack Client system.

2. (32-bit operating systems only) Start FastBack Mount by going to the Microsoft Windows taskbar area and clicking the FastBack Mount icon. The taskbar area is also called the system tray.

3. (64-bit operating systems only) Start FastBack Mount by selecting **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Mount**.

4. In the FastBack Mount window, select the repository to use as the source. By default the local repository is selected. You can select a network-shared source.

   If you do not see the repository in the list, select **Browse for folder** to go to and select a volume.

   When you connect to a shared folder with the repository volume, use the following format when you enter credentials:

   - For non-domains, *systemname\username*, then type the corresponding Microsoft Windows password.
   - For domains, *domainname\username*, then type the corresponding Microsoft Windows password.

   If you want to unload an open repository, click **Remove**.

5. To refresh data that is displayed according to the repository that is selected, click **Refresh**.

6. (Optional) To change the caching options, click **Settings**. You can select the following options:

   Enable
   > Caching is enabled. Caching is not required for local, SAN, and shared repositories.

   Access Auto-check
   > Select **Access autocheck** to gray out all the snapshots where the current user does not have permissions.

7. Select a policy. The list includes all policies that apply to the repository that you selected.

8. Select a server. The list includes servers that are backed up per the selected policy.

9. Select a volume. The list includes volumes that are backed up on the selected server. Choose the volume that has the copy of the file that you want to restore.

10. Select a date. The list includes snapshots that ran for a selected volume. You can select a specific snapshot or, at the end of the list, select the `Last Snapshot` option. The `Last Snapshot` option mounts the snapshot that is last on the list when the volume is mounted. If you mount the last snapshot, if a new snapshot completes on the same volume, the mounted volume is not automatically updated.

11. Click **Mount**.

12. In the Choose mount destination window, select a drive where you want the data to be mounted and click **OK**.

13. Open Windows Explorer. The volume mounted to the drive you selected is displayed.

14. Open a second Windows Explorer window. Go to the drive where you want to restore the files.

15. From the Windows Explorer window with the mounted volume, select the files to restore. Drag-and-drop the files to the second Windows Explorer window, to the drive where to restore the files. Verify that the size of the target is equal to, or greater than the size of the files to be restored. Otherwise, the file recovery process does not complete.

Instant Restore (Windows)

Tivoli Storage Manager FastBack can also restore volumes with instant restore. Unlike a regular volume restore, instant restore allows access to volume contents while the restore process is in progress. Less downtime is required before a recovered volume can be used because, after you start an instant restore, you can use data on the disk while the restore is in progress.

About this task

To start an instant restore, complete the following steps:

Procedure

1. Log on to the FastBack Client system with administrator credentials. FastBack Mount is installed on the FastBack Client system.

2. (32-bit operating systems only) Start FastBack Mount by going to the Microsoft Windows taskbar area and clicking the FastBack Mount icon. The taskbar area is also called the system tray.

3. (64-bit operating systems only) Start FastBack Mount by selecting **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Mount**.

4. In the FastBack Mount window, select the repository to use as the source. By default the local repository is selected. You can select a network-shared source.

   If you do not see the repository that you want to choose in the list, select **Browse for folder** to go and select a volume.

   When you connect to a shared folder with the repository volume, use the following format when you enter credentials:

   • For non-domains, *systemname\username*, then type the corresponding Microsoft Windows password.

   • For domains, *domainname\username*, then type the corresponding Microsoft Windows password.

   If you want to unload an open repository, click **Remove**.

5. To refresh data that is displayed according to the repository that is selected, click **Refresh**.

6. (Optional) To change the caching options, click **Settings**. You can select the following options:

   Enable

   > Caching is enabled. Caching is not required for local, SAN, and shared repositories.

Access Auto-check

Select **Access auto-check** to gray out all of the snapshots where the current user does not have permissions.

7. Select a policy. The list includes all policies that apply to the repository that you selected.

8. Select a server. The list includes servers that are backed up within the selected policy.

9. Select a volume. The list includes volumes that are backed up on the selected server.

10. Select a date. The list includes snapshots that ran for a selected volume. You can select a specific snapshot or, at the end of the list, select the `Last Snapshot` option. The `Last Snapshot` option mounts the snapshot that is last on the list when the volume is mounted. If you mount the last snapshot, if a new snapshot completes on the same volume, the mounted volume is not automatically updated.

11. Click **Restore**.

12. A window is displayed. The message indicates that you must stop the FastBack Client service. Stop the FastBack Client service.

13. Click **Resume**. The restore process continues.

14. In the Select Drive Letter for Instant Restore window, select a volume where you want the data to be restored and click **OK**. Verify that the size of the target is equal to, or greater than the size of the volume to be restored. Otherwise, the instant restore process does not complete.

   Attention:

   - Restoring a volume to a viewable storage volume involves overwriting data on that existing storage volume. After the restore begins, the current volume contents are permanently erased. Before you start the restore, verify that the correct volume is selected, and that there are no open handles or processes that are using that volume.

   - The restore operation fails if there are open files or applications that are running on the target restore volume. Selecting **Ignore open handles on the destination volume** causes Tivoli Storage Manager FastBack to ignore the open files and applications that are running on the destination volume. This situation can cause a problem with applications and loss of data in files that are open on the target volume.

15. A confirmation message is displayed. Click **Yes**. The restore process begins. In the Instant Restore section, you can see the status of the restore process.

Results

For the **Max CPU** control, after the Instant Restore section, you can move the slider to adjust the processor usage for the restore process.

If you want to cancel the restore process, select the instant restore session that is in progress and click **Abort**. All data on the target drive is lost. You can click **Abort All** to cancel all processes. If someone cancels or stops an instant restore session without clicking **Abort** or **Abort all**, for example, if someone stops the FastBack Mount service, the restored volume is displayed as a valid volume, but the data on the volume is invalid. The data is invalid because the data was partially restored, but the restore process did not have time to complete and the shutdown was abnormal.

If there is a temporary problem that prohibits the session from running, the instant restore session pauses. You cannot manually pause a session. The software issues a command to pause the system when a problem is detected and that problem seems to be temporary. For example, if there is a network problem that results in a temporary loss of access to the remote repository, the instant restore session pauses. To continue to the restore process after it was paused, select the appropriate line in the instant restore list and click **Resume**.

What to do next

You can use instant restore to restore a simple volume on a dynamic disk. This restore might cause the disk status to change to *Online (Errors)* and the status of all volumes on the disk to change to *At Risk*. This change in disk status can occur when network traffic is too heavy for instant restore to operate. In this situation, the volumes are online and mounted. You can return the disk and volume status to normal by going to the Computer Management Console. Right-click the disk; then, click **Reactivate Disk**.

Note: Instant restore is not supported for FastBack Server repository data on Tivoli Storage Manager tape media. For more information, see "Volume and file recovery" on page 124.

Instant restore for Microsoft Cluster Server (Windows only)
Before you begin

When running an instant restore in a Microsoft Cluster Server (MSCS) environment, data loss can occur in either of the following scenarios:
* Cluster node where the instant restore runs crashes during the restore.
* Cluster server restarts during the instant restore.

In these scenarios, the instant restore cannot be resumed. The instant restore must restart from the beginning. All new data written by the application during the restore process is lost.

About this task

To manage the MSCS environment as part of restoring a cluster volume by using instant restore, complete the following steps:

Procedure
1. To configure the cluster to not allow failover of the disk that you are restoring to, complete the following steps:
   a. Double-click the icon for the disk that contains the volume that you want to restore.
   b. Select the General tab.
   c. Click **Modify**. This button is next to the Possible Owners field. The Modify Possible Owners window is displayed.
   d. In the Modify Possible Owners window, move all nodes, except for the node that currently owns the disk, to the Available Nodes window.
   e. In the Modify Possible Owners, click **OK**.
   f. On the General tab, click **OK**.
   The cluster cannot remove the disk from the node.

2. To prevent the instant restore volume unmount from causing the resources to fail, right-click the disk; then, click **Take Offline**. All resources that are disk-dependent are automatically taken offline.

3. Use the following procedure to change the `Looks Alive` and `Is Alive` poll intervals for the disk to prevent cluster intervention during the instant restore:

   a. Double-click the disk.

   b. Select the Advanced tab.

   c. For both `Looks Alive` and `Is Alive` parameters, select the radio button to specify value.

   d. Take note of the current value for the `Looks Alive` and `Is Alive` parameters. These parameters are required for restoring it back when the restore is complete.

   e. Change the `Looks Alive` and `Is Alive` poll interval value to *604800000*. This change means that the cluster does not attempt to check the disk with these procedures for one week.

   f. Click **OK**.

4. To bring the disk online, right-click the disk icon and select **Bring online**. This action causes only the disk to go online.

5. Wait 60 seconds to ensure that the cluster validates the disk before starting the instant restore.

6. Start the instant restore.

7. To bring the other disks online after the restore starts, right-click the icon for the group that contains the disk; then, click **Bring Online**.

8. After the instant restore is complete, use the following steps to reconfigure the cluster to allow failover of the disk that you restored. This step reverses the action that you completed in step 1 on page 131.

   a. Double-click the icon for the disk that contains the volume that you want to restore.

   b. Select the General tab.

   c. Click **Modify**. This button is next to the Possible Owners field. The Modify Possible Owners window is displayed.

   d. In the Modify Possible Owners window, move all nodes to the Possible Owners window.

   e. In the Modify Possible Owners window, click **OK**.

   f. On the General tab, click **OK**.

9. Use the following procedure to restore the `Looks Alive` and `Is Alive` poll intervals of the disk back to the original values:

   a. Double-click the disk.

   b. In the displayed window, select the Advanced tab.

   c. For both `Looks Alive` and `Is Alive` parameters, use one of the following steps:

      • If the **Use value from resource type** button was selected before changing the value, select it again.

      • If the **Specify value** radio button was selected before changing the value, restore the value to the original value.

10. Resume normal operation.

Instant restore for Veritas Cluster Server (Windows only)

To manage the Veritas Cluster Server (VCS) environment as part of restore a cluster volume by using instant restore, complete one of the following procedures.

About this task

The first option is a simpler procedure that does not support the cluster to move a service group or resource between nodes during the instant restore. The service group and resource cannot move between nodes because all nodes, except for the node that contains the disk, are frozen during the instant restore.

The second option is more complicated, but the procedure does not freeze nodes throughout the instant restore. The nodes are frozen only during the instant restore initiation phase. The service group that manages the disk is also frozen until the instant restore is complete.

Option 1: Simple procedure

1. Complete the following steps to configure the cluster to not failover to the disk that you are restoring. These steps are to be completed from the Veritas Cluster Manager user interface.

   a. In the left vertical panel, select the **Systems** tab.

   b. For every node that is not the current owner of the disk that you want to restore, right-click the icon for the required node and select **Freeze** > **Persistent**. The cluster cannot remove the disk from the currently owned node.

2. Complete the following steps to take all disk-dependent resources offline to prevent the instant restore volume unmount from causing them to fail.

   a. In the left vertical panel you used in step 1, select the **Service Group** tab.

   b. Right-click the icon for the service group that contains the disk and select **Offline** *node name where the service group is online*. The service group is taken offline.

   c. Ensure that the service group is expanded in the console. If the service group is not expanded, click the **+** icon that is located next to the service group icon.

   d. Right-click the VMDg resource that manages the disk and select **Online** *the node that was online before*. The resource is online.

   e. If you are using a MountV resource to mount the volume that you want to restore, bring it online. This step is required so Windows connects the volume with a volume letter that is needed for the instant restore.

3. Start the instant restore.

4. Right-click the icon for the service group that contains the VMDg that manages the disk and select **Online** *the node that was online before*. The service group is online.

5. After the instant restore is complete, use the following steps to reconfigure the cluster to support failover to the disk that you restored. This step reverses the task that you completed in 1.

   a. In the left vertical panel, select the **Systems** tab.

   b. For every node that is not the current owner of the disk that you restored, right-click the icon for the required node and click **Unfreeze**.

   c. The cluster can remove the disk from the node.

6. Resume normal operation.

Option 2: Advanced procedure for improved performance

1. Complete the following steps to configure the cluster to not failover to the disk that you are restoring. These steps are to be completed from the Veritas Cluster Manager user interface.

   a. In the left vertical panel, select the **Systems** tab.

   b. For every node that is not the current owner of the disk that you want to restore, right-click the icon for the required node and select **Freeze** > **Persistent**. The cluster cannot remove the disk from the currently owned node.

2. Complete the following steps to take all disk-dependent resources offline to prevent the instant restore volume unmount from causing them to fail.

   a. In the left vertical panel you used in step 1, select the **Service Group** tab.

   b. Right-click the icon for the service group that contains the disk and select **Offline** *node name where the service group is online*. The service group is taken offline.

   c. Ensure that the service group is expanded in the console. If the service group is not expanded, click the **+** icon that is located next to the service group icon.

   d. Right-click the VMDg resource that manages the disk and select **Online** *the node that was online before*. The resource is online.

   e. If you are using a MountV resource to mount the volume that you want to restore, bring it online. This step is required so Windows connects the volume with a volume letter that is needed for the instant restore.

3. Start the instant restore.

4. After the instant restore starts, you can bring the service group online. To bring the service group online, right-click the icon for the service group that contains the VMDg that manages the disk. Select **Online** *name of the node where the service group was online*.

5. Right-click the service group icon and select **Freeze** > **Persistent** to freeze the service group that contains the disk.

6. Complete the following steps to unfreeze the frozen nodes. This step reverses the task that you completed in 1.

   a. In the left vertical panel, select the **Systems** tab.

   b. For every node that is not the current owner of the disk that you restored, right-click the icon for the required node and click **Unfreeze**.

   c. The cluster can move all resources except for the service group that contains the VMDg that manages the disk.

7. After the instant restore is complete, right-click the service group icon and select **Unfreeze** to unfreeze the service group that contains the disk.

8. Resume normal operation.

File-level restore and instant restore (Linux)

FastBack Mount on Linux is used to restore individual files (file-level restore) or volumes (instant restore). Unlike a regular volume restore, instant restore allows access to volume contents while the restore process is in progress. Less downtime is required before a recovered volume can be used because, after you start an instant restore, you can use data on the disk while the restore is in progress.

About this task
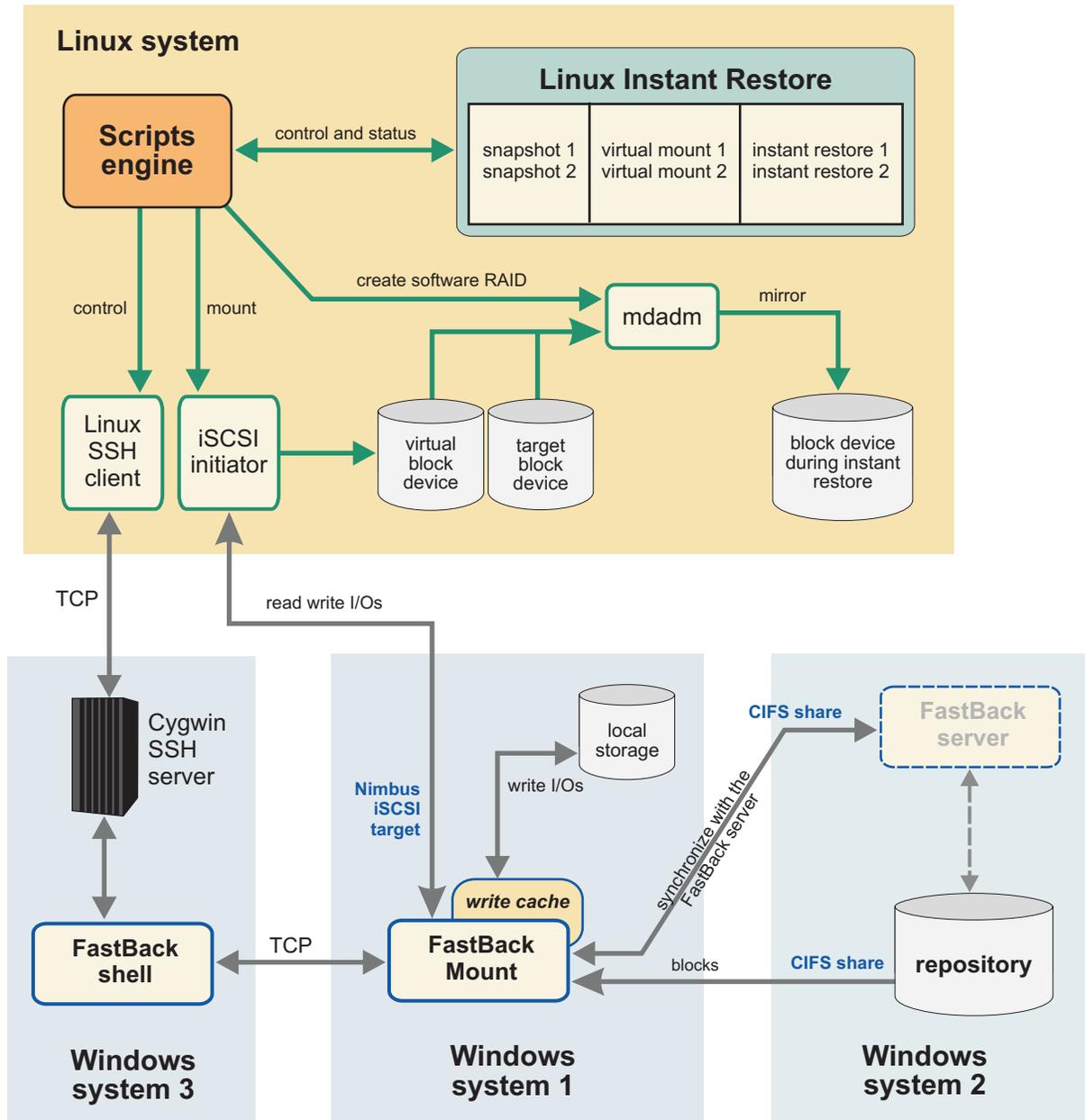
Figure 8. Linux Instant Restore

Figure 8 shows all the modules that work together to provide FastBack Mount on Linux. It allows the FastBack Shell (Windows system 3) and FastBack Mount (Windows system 1) to connect to multiple repositories (Windows system 2). Snapshots on these repositories are available for file-level recovery or instant restore operations.

Table 24. Minimum environment for Linux instant restore

System:	Must contain these applications:
Linux system	• FastBack Client • FastBack Mount

Table 24. Minimum environment for Linux instant restore (continued)

System:	Must contain these applications:
Microsoft Windows system	• FastBack Server • FastBack Shell • FastBack Mount • Secure Shell (SSH) key authentication to the Linux system

Table 25. Example Windows environment for Linux instant restore

System:	Runs these applications:
Microsoft Windows system #1	FastBack Server
Microsoft Windows system #2	FastBack Mount
Microsoft Windows system #3	• FastBack Shell • Secure Shell (SSH) key authentication to the Linux system

Table 26. Minimum package requirements for Linux instant restore

Packages:	Minimum version:
open ssh	0.10
mdadm	2.6
lsscsi	0.10
iscsiadm	2.0

Note: If the minimum package versions are not installed, the following message is displayed:

```
WARNING: One of the tools is missing or with wrong version.
Check the logs in
/opt/IBM/Tivoli/TSM/FastBack/mount/engine/var
```

Configuring FastBack Mount for restore operations

FastBack Mount requires specific application settings, environment conditions, and configuration tasks be completed before you attempt a restore operation.

Before you begin

These environment requirements must exist before you use FastBack Mount on Linux:

• Tivoli Storage Manager FastBack Administrative Command Line must be available on a Windows computer. Secure Shell (SSH) Server must be installed on this computer and accessible to the SSH client that is installed on the Linux target system. The Administrative Command Line is also called the FastBack Shell.

• FastBack Mount is available on a Windows system. This system must be accessible from the computer where FastBack Shell is installed. Alternatively, FastBack Mount and FastBack Shell can be installed on the same computer.

• FastBack Mount must be able to access the FastBack repository. FastBack Mount exposes FastBack snapshots as iSCSI targets. Therefore, the repository snapshots must be accessible to the target Linux system. Access the repository by

configuring Common Internet File System (CIFS) shares to the FastBack Mount applications or by installing FastBack Mount on the computer that hosts all repository locations.

- Make sure that your environment consists of all prerequisite applications as described in "FastBack Mount" on page 19.
- FastBack Mount saves changes to data on a virtual volume in the write cache. The write cache is enabled by default, the path is `C:\Documents and Settings\All Users\Application Data\Tivoli\tsm\FastBack\mount`, and the size is set to a maximum of 90% of the available space. These settings can be configured by clicking settings in the main FastBack Mount window, or by editing the configuration file `FastBackMount.conf`. The write cache must be on a local drive and cannot be set to a path on a shared folder. If the write cache is disabled, changes to the data on a virtual volume are stored in RAM.
- It is possible to unmount the virtual device on the Linux system when you mount a snapshot. However, unmount causes an automatic recovery process to mount the device again.
- To prevent the recovery process from mounting the device, stop the cron daemon. For example:

```
(RedHat)
/etc/init.d/crond stop
```
```
(SUSE)
/etc/init.d cron stop
```

Make sure to start the cron daemon when processing completes.

About this task

This task guides you through configuration steps that are required to use FastBack Mount.

Procedure

1. Log on to the Linux system (where the FastBack Client is installed) with root user authority. FastBack Mount must be installed on this FastBack Client Linux system.
2. Start FastBack Mount by clicking the FastBack Mount icon on the desktop or running a script from the shell prompt. The first time that you access FastBack Mount, the Settings dialog displays. You must enter the following configuration information to proceed:
   - **FastBack Shell**
     a. Enter the host name or IP address of the computer where FastBack Shell is installed.
     b. Enter the login ID that is used for the Secure Shell (SSH) user.

        Tip: This login ID is for the Windows system where both FastBack Shell and SSH are installed. This system uses SSH to communicate with FastBack Mount on the Linux system. Make sure that this login ID uses a host name convention that is defined in the SSH known_hosts file. For more information, see Step 4f in "Administrative Command Line (Linux only)" on page 33.
   - **FastBack Mount**
     Enter the host name or IP address of the Windows system where FastBack Mount is installed. Click **OK** to save these values and return to the FastBack Mount window.

These settings are stored in the FastBackMount.cfg file.

3. Use the Select a repository drop-down menu to identify the repository to use as the source:

   - To use an existing repository, click the repository. Your selection is saved and you return to the FastBack Mount window. Click **Refresh** to display the most current repository data.

   - To add a repository, click `Add a repository` in the drop-down menu. Choose from one of the following two repository locations in the Add a repository dialog:

   `Repository on remote share`
   Select this value to use a repository that is on a Windows system within your environment. Enter the following information:

   – **Credentials to connect to your repository**

      a. Enter the login ID that is used for this Windows system.

      b. Enter the password for this login ID.

      c. Enter the domain to which the login ID belongs.

   – **Input your repository location**
   Enter your repository location. For example:

   ```
   \\vm-03ent-test3.mycompany.com\REP
   ```

   Important: For Linux systems, a Windows share is mounted by using the forward slash character (/). However, for FastBack Mount on Linux, the backslash character (\) is required to mount the repository.

   `Repository on TSM server`
   Select this value to use a repository that is on a Tivoli Storage Manager server. The Tivoli Storage Manager server must already be configured and accessible to FastBack Mount. Enter the following information:

   – **Input TSM server address**

      a. Enter the IP address or host name of the Tivoli Storage Manager server.

      b. Enter the port number that is used for TCP/IP communication with the server.

   – **Input TSM server credentials**

      a. Enter the node name that is used to access the Tivoli Storage Manager server.

      b. Enter the password that is associated with the node name.

      c. Enter the `asnodename`. This name is similar to the previously entered node name. However, the `asnodename` provides proxy authority for your Linux system to back up and restore data to the Tivoli Storage Manager server.

   – **Branch name**
   Enter the branch name of the FastBack Server on the FastBack Disaster Recovery Hub.

   Click **OK** to save these values and return to the FastBack Mount window.

   Click **Refresh** to display the most current repository data.

Results

FastBack Mount is now properly configured and ready for restore operations.

What to do next

Use FastBack Mount to accomplish a file-level restore or an instant restore operation.

File-level restore on Linux
Before you begin

Be aware of these considerations before you attempt a file-level restore on Linux:

- The destination partition is available for both read-only or read/write modes.
- The tasks that are described in Configuring FastBack Mount must be completed before you attempt a file-level restore.
- This procedure assumes that you are logged on to the Linux system (where the FastBack Client is installed) with root user authority and the FastBack Mount GUI is available.
- SUSE Linux Enterprise Server 10 requires all iSCSI devices to be unmounted before rebooting or shutting down the system.
- File-level recovery is not supported for FastBack Server repository data on Tivoli Storage Manager tape media. For more information, see "Volume and file recovery" on page 124.

About this task

This task guides you through how to use FastBack Mount to restore files on a FastBack Client Linux system.

Procedure

1. Identify the snapshot to restore in the **Select snapshot** field:
   a. Select a policy. All Linux policies that apply to the selected repository are available.
   b. Select a server. All servers that are backed up within the selected policy are available.
   c. Select a volume. All volumes that are backed up on the selected server are available.
   d. Select a date. All snapshots that ran for a selected volume are available. You can select a specific snapshot or, at the end of the list, select the Last Snapshot option. The Last Snapshot option mounts the snapshot that is last on the list when the volume is mounted. If you mount the last snapshot, if a new snapshot completes on the same volume, the mounted volume is not automatically updated.
2. Click **Mount**. The Choose Mount Destination window displays:
   a. Specify the mount point for the target.

      Tip: The mount point identifies a *volume*.
   b. Specify whether to mount the volume in read only or read/write mode. All write operations that are applied to the mounted volume are lost after unmount when mounted in read/write mode.
   c. Click **OK** to close the Choose Mount Destination window.

Results

If your file-level restore completed successfully, a new entry displays in the **Mounted Volumes** field. For example:

```
testPolicy is mount of [\\vm-03ent-test3.mycompany.com\REP]-
[Policy 0-vm-rh5u2-64-dev4-/sdb1 at 2010-Mar-24 10:15:50
```

Instant restore on Linux
Before you begin

Be aware of these considerations before you attempt an instant restore on Linux:

- The Windows FastBack Server and FastBack Shell components must be installed in the default path. Also, the default path must contain English language characters only.
- The destination partition is available for both read-only or read/write modes.
- Multiple instant restore sessions to different target disks run in parallel. However, multiple instant restore sessions to different target partitions on the same disk do not run in parallel. As a result, the first instant restore session must complete before the next instant restore session begins.
- The tasks that are described in Configuring FastBack Mount must be completed before you attempt an instant restore.
- This procedure assumes that you are logged on to the Linux system (where the FastBack Client is installed) with root user authority and the FastBack Mount GUI is available.
- SUSE Linux Enterprise Server 10 requires all iSCSI devices to be unmounted before you restart or shut down the system.
- Instant restore to LVM partitions is not supported.
- Instant restore is not supported for FastBack Server repository data on Tivoli Storage Manager tape media. For more information, see "Volume and file recovery" on page 124.
- If the destination volume is written to during an instant restore, a write cache must be used. The size of the write cache must be large enough to accommodate the write operation.

About this task

This task guides you through how to use FastBack Mount to restore a snapshot volume (instant restore) on a FastBack Client Linux system.

Procedure

1. If this is the first instant restore to the device, skip this step and proceed to Step 2. If this device was used for a previous instant restore, you must unmount and shut down the RAID that contains the target device as shown:

   a. Issue this command to unmount the volume:

      umount /dev/mdx

   b. Issue this command to shut down the RAID:

      mdadm --stop /dev/mdx

      Where mdx is the disk that contains the target device.

2. Identify the snapshot to restore in the **Select snapshot** field:

   a. Select a policy. All Linux policies that apply to the selected repository are available.

   b. Select a server. All servers that are backed up within the selected policy are available.

c. Select a volume. All volumes that are backed up on the selected server are available.

d. Select a date. All snapshots that ran for a selected volume are available. You can select a specific snapshot or, at the end of the list, select the `Last Snapshot` option. The `Last Snapshot` option mounts the snapshot that is last on the list when the volume is mounted. If you mount the last snapshot, if a new snapshot completes on the same volume, the mounted volume is not automatically updated.

3. Click **Restore**. The Select Mountpoint or Block Device for Instant Restore window displays:

a. Specify the mount point for the instant restore target. The mount point identifies a *volume*. Verify that the size of the target is equal to, or greater than the size of the volume to be restored. Otherwise, the instant restore process does not complete.

   Attention: Restoring a volume to a viewable storage volume involves overwriting data on that existing storage volume. After the restore begins, the current volume contents are permanently erased. Before you start the restore, verify that the correct volume is selected, and that there are no open handles or processes that are using that volume.

b. Specify the block device for the instant restore target. The block device identifies a *physical device*.

   Tip: Although only one value is required, it is advised to specify both a mount point and a block device.

c. Click **OK** to close the Select Mountpoint or Block Device for Instant Restore window.

The instant restore session begins. During the instant restore operation, the content of the restored volumes is available for access.

What to do next

Backing up a restored volume:
If you plan to back up a restored volume, you must complete either of the following two actions before you attempt a backup operation:

* Restart the Linux system where the FastBack Client is installed.
* Manually stop the mirror device and mount the restored volume.

   For example, in the following procedure, `sdc1` is the target block device and `md0` is the mirror device:

   1. Issue the command: `umount /dev/md0`.
   2. Issue the command: `mdadm --stop /dev/md0`.
   3. Issue the command: `mount /dev/sdc1 /restoredVolume`.

Checking the file system
Before you run a file system check (with the `fsck` file system utility) after the instant restore completes, complete these tasks:

1. Unmount the RAID device by issuing this command: `umount /dev/md0`
2. Type in the `fsck` command to run the file system check.

Continuous Data Protection (Windows only)

Normal snapshots record backup data at a certain point in time. Continuous Data Protection records all the activity, even activity that occurs between snapshots.

If enabled, Continuous Data Protection supports data restore to any specific point after the last snapshot, and between the last snapshot and the one before last on the same chain. The following list provides information that you need to know before enabling Continuous Data Protection:

- Continuous Data Protection is not supported for dynamic disks.
- With Continuous Data Protection, Tivoli Storage Manager FastBack restores a volume to a point in time based on the writes occurring to the volume a the time of Continuous Data Protection point-in-time placement. Because FastBack Mount and instant restore rely on incremental snapshots, Continuous Data Protection cannot be used with either FastBack Mount or instant restore. For more information about restoring snapshots that include Continuous Data Protection, see "Restoring data from Continuous Data Protection snapshots (Windows only)."
- Using Continuous Data Protection requires additional processor, memory, and network bandwidth resources. The amount of additional hardware required depends on the server activity.
- Running defragmentation on volumes protected with Tivoli Storage Manager FastBack Continuous Data Protection generates a significant load on the server running Continuous Data Protection, in addition to large incremental snapshots, and might result in failure.

  For the supported Windows 2008 and Windows Vista operating systems, the defragmentation task runs automatically on all volumes. To disable the defragmentation task, open the Task Scheduler. You can open the Task Scheduler from the Windows Start menu. Click **Programs** > **Accessories** > **System Tools** > **Task Scheduler**. Navigate to **Task Scheduler (local)** > **Task Scheduler Library** > **Microsoft** > **Windows** > **defrag**. From this window, disable the `ScheduledDefrag` task.
- Do not run Continuous Data Protection on system volumes.

When Continuous Data Protection is enabled, adhere to the following rules:

1. Make sure that Tivoli Storage Manager FastBack repository disks and folders are excluded from any file-level scanning, for example, anti virus and anti spyware software.
2. Continuous Data Protection snapshots should be scheduled every hour.

While using Continuous Data Protection gives you the ability to restore a system to a point in time, choosing a proper time point can be a complex decision. This task is simplified by adding log events of the FastBack Client operating system application to the Continuous Data Protection slider layout. Because there are many application log events, these events can be filtered by an external script on the FastBack Server. For more information about filtering these events, see "Continuous Data Protection slider and FastBack Server events (Windows only)" on page 144.

Restoring data from Continuous Data Protection snapshots (Windows only)

About this task

Before you restore data from Continuous Data Protection snapshots, review the following notes:

Notes:

- Snapshots with Continuous Data Protection data are marked with the icon.
- Snapshots marked with an icon indicate a completed Continuous Data Protection snapshot, but a segment of the Continuous Data Protection data might be missing. This icon indicates that when you open the details for this snapshot, some periods are marked red and unavailable for restore. You can restore other Continuous Data Protection periods. If the volume is small and a small segment of data is missing, the icon might not be displayed.
- If a Continuous Data Protection snapshot is still running, the following icon is displayed: .
- To view the size of the Continuous Data Protection data, right-click the wanted snapshot in the Snapshots Monitor window and select **Properties**.

Overview of Continuous Data Protection icons:

Table 27. Continuous Data Protection icons

Continuous Data Protection icons	Description
	Continuous Data Protection Snapshot is running.
	Continuous Data Protection Snapshot completed successfully.
	Incomplete Continuous Data Protection snapshot, the Continuous Data Protection data before the terminating point might be available.

- To restore Continuous Data Protection data between the last snapshot and the one before last, select a completed Continuous Data Protection snapshot.
- To restore Continuous Data Protection data that is recorded after the most recent snapshot is complete, select a currently running Continuous Data Protection snapshot.

To restore a Continuous Data Protection snapshot, complete the following steps:

Procedure

1. Click **Snapshots Monitor**.
2. Right-click a Continuous Data Protection snapshot; then, click **Restore** > **Continuous Data Protection Volume Restore**.

   Note: Only the last two Continuous Data Protection snapshots from each chain are available in the **Snapshots Monitor** list.
3. In the displayed window, select a destination volume and click **Next**.
4. Close any applications that are running on the destination volume. The restore operation fails if there are applications that are running or files open on the target restore volume. If you select **Ignore open handles on the destination volume**, Tivoli Storage Manager FastBack ignores files that are open and applications that are running on the destination volume. Files that are running and applications that are running can cause a problem with the target volume. You must close the files and applications that are open on the destination volume. Use the **Ignore open handles on the destination volume** only if there is no other choice.
5. Click **Next Step**.

6. The window contains a scale that represents the time between two snapshots (Continuous Data Protection range).
   - Events that took place during that time are marked as green lines.
   - Consistency points within that range are marked blue.
   - Hovering over an event or a consistency point shows a tooltip that indicates the event/consistency point name.
   - Parts of the Continuous Data Protection range that are marked with broken red line are periods within the Continuous Data Protection range, in which no activity was registered because the server was not available because of network issues. These periods cannot be restored by using the Continuous Data Protection feature. To restore the data, covered by the red area, use the next consistent snapshot.

7. Move the sliding dial to the point where you want to restore.

   The time and date are indicated in the time and date fields under the time line. You can also enter the time in the time field. If the time field contains the valid Continuous Data Protection restore time, its font color is black. Otherwise, it is red. The date field is disabled and can be changed only by moving the dial when the range for the scale exceeds one day.

   If you select **Restore to consistency points or events only**, the dial snaps to the closest event or consistency point so you can restore to consistency points or events.

8. Click **Restore**. The point that you selected is restored to the destination volume you specified. **Restore** is enabled only when a valid restore time is selected.

Stopping Continuous Data Protection (Windows only)

Continuous Data Protection is stopped automatically in the following cases and then restarted at the beginning of the next scheduled snapshot:
- When FastBack Client or FastBack Server is restarted.
- When there is a communication problem between the FastBack Client and FastBack Server.
- When there is strong resource contention on the host. This limit is controlled by the `FastBackClient.ini` file.
- When another snapshot in the same chain starts Continuous Data Protection.
- By default, when a third Continuous Data Protection snapshot is started, the data of the first Continuous Data Protection snapshot in the same chain is deleted.

To terminate Continuous Data Protection while it is running, go to the Snapshot Monitor, right-click the wanted snapshot, and select **Immediate operations** > **Abort CDP**. This option is only available if the selected snapshot is running Continuous Data Protection.

The next snapshot in the chain includes Continuous Data Protection unless you clear the check box from the relevant job schedule.

Continuous Data Protection slider and FastBack Server events (Windows only)

Using the Continuous Data Protection slider, a green mark indicates the event that occurred on the FastBack Client. For example, the event can be the discovery of a virus. With this information you can decide when to restore the volume. In this example, you can restore data to the time before the virus affected the system.

The events are extracted by FastBack Server every time a CDP slider layout is created. FastBack Server creates a file named `ContinuousEventsInOut.txt` that contains all the time-relevant events for the particular snapshot with continuous data protection. The file is located in `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\Server\ContinuousEventsInOut.txt`.

This file can be filtered and integrated into the information sent to the FastBack Manager. The events listed in this file are displayed by the FastBack Manager as green marks on the CDP scale.

Note: For the events mechanism to work properly, the currently logged user on the FastBack Server system must have sufficient permissions to access the log events located on the FastBack Client.

If there are permission restrictions, the CDP restore window might not open. You can cancel the extraction of events from the FastBack Client. Events extraction can be canceled at run time by creating a file in the following directory: `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\Server\ DoNotAddEventsToJavaContinuousLayout`

Reminder: It can take as many as 30 seconds for FastBack Server to detect the file.

Events filtering mechanism (Windows only)

When FastBack Server creates the file `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\server\ContinuousEventsInOut.txt`, and before it sends it to FastBack Manager, FastBack Server tries to start a script at `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\ server\FilterContinuousEventsScript.bat`.

FastBack Server passes the path to `ContinuousEventsInOut.txt` in an environment variable called *%EventsFileName%*. This variable can be used inside the script to filter the events. Check the content.

If the batch file is not present, the default is present, the `ContinuousEventsInOut.txt` file is passed to FastBack Manager as is.

For example, the batch file, `ContinuousEventsInOut.txt`, contains a single line:

```
echo %EventsFileName% > out.txt
```

In this case, when the Continuous Data Protection slider window is opened, a file named out.txt is created in the FastBack Server executable directory. This file contains a single line; the result of the echo command:`C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\server\ ContinuousEventsInOut.txt`.

Notes:
- One of the limitations of this mechanism is that the size of the filtered `ContinuousEventsInOut.txt` file is not to exceed the size of the original file. This means that the script is to remove only the events, but not add anything new.
- Any output to the screen, for example, the echo specified in the script, is lost because the script does not have a window to show the output. However, output to files works and if no path is specified the files are searched in the FastBack Server executable directory only and not in the `Documents and Settings` directory.

Packaging (Windows only)

Events and filtering mechanism are already part of FastBack Server service and do not require any special installation.

The reference implementation of Oracle9i SCN number extraction to the Continuous Data Protection slider is packaged as a batch script called `C:\Program Files\Tivoli\TSM\FastBack\client\scripts\Oracle9i_GetSCNNumber.bat`.

To run the `Oracle9i_GetSCNNumber.bat` script that is in the `C:\Program Files\Tivoli\TSM\FastBack\client\scripts\` directory, complete the following steps:

1. Open the **Scheduled Tasks** control panel and use the wizard to create a scheduled task that runs the `C:\Program Files\Tivoli\TSM\FastBack\client\scripts\Oracle9i_GetSCNNumber.bat` script daily. The content is to be changed and related system variables is to be updated.
2. In the final window of the Scheduled Tasks wizard, select **Open advanced properties**. Alternatively, in the Scheduled Tasks folder, right-click the task you created and select **Properties**.
3. Select the **Schedule** tab.
4. Click **Advanced**.
5. Enable **Repeat task**.
6. Select **Every 5 minutes**, and **Duration: 24** hours.
7. Go to the Windows Event Viewer, and check the resulting events. Verify that a new event is created every 5 minutes.
8. Right-click an event and select **Properties** to view the event details.

To add an event to the Event Viewer, use the `eventcreate.exe` command line utility.

Microsoft Exchange back up and restore

Tivoli Storage Manager FastBack provides point-in-time copies of Exchange 2000, Exchange 2003, Exchange 2007, and Exchange 2010 databases and transaction logs, without compromising either data integrity or performance of online operations.

You can use Individual Mailbox Restore (IMR) to implement an individual mailbox restore for public folders. The IMR support is provided on an as-is basis.

Combined with Tivoli Storage Manager FastBack for Microsoft Exchange, Tivoli Storage Manager FastBack enables restoring attachments, emails, folders, mailboxes, databases, and entire servers.

Background

Exchange 2000, 2003, and 2007 are based on the concept of partitioning the database into storage groups defined by the user. On Exchange 2000 and 2003, up to four storage groups can be defined, where each storage group can contain a maximum of five databases for a maximum of 20 databases per server. On Exchange 2007, up to 50 storage groups can be defined and up to 50 databases. Exchange is a transaction-based email system in which database transaction integrity is defined by Atomicity, Consistency, Isolation, and Durability.

Exchange Server 2010 does not include this concept of partitioning the database into storage groups defined by the user. Instead, Exchange 2010 considers the database as a stand-alone component. Each database still has its own transaction

log and checkpoint file. A maximum of 100 databases can be connected to each Exchange 2010 server. In addition, Exchange 2010 uses database availability groups (DAG). A DAG consists of mailbox servers that provide recovery from database, server, or network failures. They provide continuous replication and continuous mailbox availability. Each database can be replicated to up to 16 Exchange 2010 servers. These replicated databases can be distributed across geographic locations. The following Microsoft document provides useful information about Exchange Server 2010 requirements: http://technet.microsoft.com/en-us/library/aa996719.aspx

Database integrity is maintained by writing each transaction to the transaction logs before it is committed to the database, and by using checkpoint files as a reference point to determine database consistency. There is one set of transaction logs for each storage group on Exchange 2000, 2003, 2007, and Exchange Enterprise systems. Transaction log names are sequentially named log files. For example, the first file would be E0000001.log, the next would be E0000002.log. On Exchange 2000 and 2003, each file has a size of 242 880 bytes. On Exchange 2007, the transaction log size is 1 048 576.

To save on disk space, Exchange provides the Circular Logging option. Circular Logging enables maintaining a number of transaction logs, typically four or five, while overwriting the oldest transaction logs.

Exchange 2007 locale continuous replication files are not backed up by Tivoli Storage Manager FastBack.

Tivoli Storage Manager FastBack for Microsoft Exchange back up and restore processes

The Tivoli Storage Manager FastBack for Microsoft Exchange back up and restore process automatically detect the version of the Exchange system installed on the server and the configured storage groups or databases.

Snapshots are taken of each selected storage group. Each snapshot consists of the *.EDB, *.LOG, *.CHK and *.STM (2000 and 2003 only) files for each storage group (Exchange 2000, 2003, and 2007) or database (Exchange 2010). The backup of the Exchange system is performed at the volume. This backup is like a regular volume backup.

Disable the circular logging option and delete unnecessary log files using the Purge Log option in FastBack Manager. After the backup is complete, the log files can be automatically erased from the primary storage (set by selecting the Purge Exchange Logs after completed snapshot in the **General configuration** > **Application** tab). The settings can also be modified per job at Job Schedule level.

Create a separate policy for each Exchange version.

Types of backup

There are two types of backup: quiescent and non-quiescent.

Quiescent backup is an offline backup. A quiescent backup results in a consistent database, but requires interrupting the operation of the server. The application is released immediately, while the backup process continues to its completion. A quiescent backup is a longer process as services are temporarily shut down to bring databases to a consistent state.

For Tivoli Storage Manager FastBack there are two types of quiescent backup: Volume Shadow Copy (VSS) service application quiescing and IBM application quiescing. You cannot use VSS application quiescing and IBM application quiescing at the same time. In addition, you cannot use VSS application quiescing to back up utility partitions.

The following list identifies scenarios when you use VSS application quiescing and IBM application quiescing:

- Use IBM application quiescing for supported Windows 2000 and Windows XP operating systems.
- Use VSS application quiescing for supported Windows 2003 and later operating systems. If you need an application-aware snapshot, do not use VSS application quiescing.
- To back up applications that run on supported Microsoft Exchange servers, verify that the VSS service is supported to take snapshots of the application.

A non-quiescent backup is an online backup. Non-quiescent backup is implemented without interrupting the operation of the server. Because server operation is not interrupted, the backup can be implemented more often. A non-quiescent backup can lead to non-consistent databases with a longer restore process and can result in some data loss. To compensate for data loss, you might want to use a more aggressive backup strategy with non-quiescent backups. Non-quiescent databases can usually be repaired by using standard Exchange tools, for example, `ISINTEG` and `ESEUTIL`. Databases that suffer from severe corruption can still be restored by using Tivoli Storage Manager FastBack for Microsoft Exchange.

To improve your chances for successful restore of both quiescent and non-quiescent backups, turn off the **Circular logging** option in System Manager.

Note: The process of migrating from Microsoft Exchange 5.5 to Microsoft Exchange 2000 while the FastBack Client is running on the migrated server is not supported. You must restart the FastBack Client after the migration.

Setting the global application aware parameters (Windows only)

About this task

The Exchange backups are defined, by default, in the global application aware parameters as *Non-Consistent*. *Non-Consistent* means no quiescing. In addition, by default, purge logs are disabled. These settings can also be changed for specific jobs as listed in the Job category.

For more information about changing global application-aware parameters, see "Application Aware options (Windows only)" on page 157.

Creating an Exchange snapshot policy

You can use the Simple Snapshot wizard to create an Exchange snapshot policy.

About this task

When two job schedules are set to run on the same volume and at the same time, the full backup job schedule takes priority and is run before an incremental job schedule. In addition, the quiescing job schedule has priority over the non-quiescing job schedule.

When running an Exchange snapshot policy, verify that the Exchange server is correctly configured. The database must not be empty and is to have volumes. An Exchange server with an empty database and no volumes does not create the agent information for the server. As a result, the FastBack Server resets itself every time the FastBack Manager tries to connect to the server. To avoid this problem, either delete the empty database, or add volumes and correctly configure the database.

To create an Exchange snapshot policy, complete the following steps:

Procedure

1. Right-click **Policies**. From the pop-up menu, click **New Policy**.
2. Select the storage groups (Exchange 2000, 2003, 2007) or database (Exchange 2010) to be backed up. The corresponding volumes are automatically selected. All data on the selected volumes is backed up. Dismounted Exchange 2007 databases are not displayed in FastBack Manager. If an Exchange Storage Group is renamed, the change is not updated in the FastBack Manager, until the Mailbox Store is dismounted and remounted.
3. For **Snapshot Every**, choose the rate at which the snapshot is taken.
4. (Optional) Select the **Exclusion** period and enter the times during the day when a backup is not to be done.
5. Click **Apply.** A new snapshot policy is created. For example, *Multi Volume Client1 Every 30 min*.
6. Click this snapshot policy to display the associated client group and job names. You can edit the snapshot policy properties.
7. Type a name for the snapshot policy.
8. **Enable DR** - Enable or disable the Disaster Recovery function for this snapshot. If enabled, all the snapshot data is replicated by the DR procedure. Do not enable DR on a policy on which CDP (Continuous Data Protection) is enabled. Enabling DR for a policy that has CDP enabled can overload the network because the CDP data is replicated by the DR process. If DR is required, add another policy with DR in lower frequency, and without CDP.
9. Set the **Number of generations** and **Snapshots Priority** (which snapshot is run first in situations in which the system capability for doing snapshots is restricted for whatever reason). The **Number of generations** is the number of snapshots that are to be retained.
10. To edit the job, select the job name and click **Go to**.
11. As necessary, modify the job name, range, and frequency.
12. Click **Advanced** and make any additional changes.
13. (Windows only) Under Application Aware, the **Quiescing** and **Purge** options are defined according to the global definitions (under the Application tab). You can change the settings for the job. To consistently back up a Microsoft SQL Server or Microsoft Exchange 2003 client, use VSS application quiescing.

    If you select an Exchange volume and EISA partition in the same policy, the Exchange logs are not deleted. To solve this problem, create two policies; one for the Exchange volume, and one for the EISA partition.

14. (Windows only) In some cases, if a database that is being backed up is spread across many volumes, the first full snapshot might not be consistent. However, the following incremental snapshots are consistent. If quiescing is selected, user exit-point scripts do not run, even if the options are selected.

    Click **OK** to close the Application Aware window.
15. Click **Apply** to save changes.
16. Change the storage groups to be backed up by editing the client group of the same snapshot policy.

Backing up a clustered Exchange file server

The clustered volume is indicated by the icon.

About this task

The FastBack Client must be installed on each node in the cluster. Using the FastBack Client, verify that the SAN Module option is enabled. For more information about using Tivoli Storage Manager FastBack in a cluster environment, see "Microsoft Cluster Server (MSCS) and Veritas Cluster Server (VCS) (Windows only)" on page 40.

To back up the clustered Exchange file server, complete the following steps:

Procedure

1. On the cluster Exchange volume, create a client group.
2. To move groups from one node to another node, use the Cluster Administrator. After moving groups, by default, the next snapshot is an incremental delta block snapshot.

Backing up an SQL server on a Microsoft cluster

The clustered volume is indicated by the icon.

About this task

The FastBack Client must be installed on each node in the cluster. Using the FastBack Client, verify that the SAN Module option is enabled. For more information about using Tivoli Storage Manager FastBack in a cluster environment, see "Microsoft Cluster Server (MSCS) and Veritas Cluster Server (VCS) (Windows only)" on page 40.

To back up an SQL server on a Microsoft cluster, complete the following steps:

Procedure

1. Install the FastBack client on each Microsoft Cluster node. Restart each node when the installation is complete.
2. Open the FastBack Client Configurator and change the SAN Module Enabled to Yes. Click Yes when prompted to restart the FastBack client.
3. Using the FastBack Manager GUI, create a new client group, and from the active node select the cluster volumes on which the SQL databases reside.

4. Change one of the passive nodes to `active` by creating a manual failover. After you change to a different active node, you can see in the Snapshots Monitor window that the policy is still running and is backing up the SQL cluster volumes.

Exchange server restore

The process for restoring Exchange server data has minor variations based on the version of Exchange server in use.

The Exchange 2000 restore procedures from inconsistent and consistent databases are the same, unless the inconsistent database is severely damaged.

An Exchange database restore can be implemented on the following systems:
- Primary server
- Backup server

If you implement an Exchange database restore on a backup server, ensure that the primary server and backup server have the same Windows and Exchange service packs and updates installed. A separate Active Directory is to also be installed. The backup server can run on the production network.

The Active Directory naming between the active server and the recovery server does not have to match. The following information for the active server and the recovery server is to match:
- Organization name
- Administrative group name
- Storage group name
- Logical database name
- `LegacyExchangeDN` names of administrative system objects

When restoring Exchange Server 2010 databases that belong to a DAG, the data must maintain consistency among the Exchange servers. The following Microsoft document provides useful information about restoring and recovering Exchange Server 2010 databases in this situation:http://msdn.microsoft.com/en-us/library/aa579420.aspx

Restoring a full Exchange 2000 Server database
Before you begin

Before you start the restore process, dismount the database used for the storage group. When you start the restore process, you have to choose the type of restore to complete. There are three different types of restore options:

Volume restore
Restore primary volume data from a copy pool or an active-data pool.

Instant restore
Data recovery is performed in the background.

Drag and drop from FastBack Mount
Mount volumes from the repository. You can view the snapshot locally, with read-only access, and on the server.

If you run a volume restore, dismount all storage groups that belong to the volume.

About this task

To restore a full database for a Exchange 2000 Server, complete the following steps:

Procedure

1. From the FastBack Client system with the Microsoft Exchange server, open the **Exchange System Manager** window.
2. In the Exchange System Manager window, expand the Servers folder.
3. Right click to select the required Exchange server and storage group; then, click **Mailbox Store** > **Dismount**. The database is not mounted.
4. From FastBack Manager window, click the **Recovery** tab.
5. To restore, use one of the following procedures:
   - To complete a volume restore, in the main window, select a snapshot. In the **Recovery** tab, click **Advanced**. For instructions to complete a volume restore, see "Restoring volumes" on page 126.
   - To complete an instant restore complete the following steps:
     a. From the Exchange server, open FastBack Mount.
     b. Select the snapshots to restore.
     c. Restore database and log volumes to your Exchange volume. If your database and logs are in different locations, restore all volumes. For example, if the database volume is on E: and the log volume is on F:, you have to locate the correct snapshots for each volume. Right-click to select the snapshots; then, click to select Instant Restore.
   - To complete a restore using drag and drop from FastBack Mount, complete the following steps:
     a. From the Exchange server, open FastBack Mount.
     b. Mount the snapshots you need for the restore.
     c. Open the mounted volumes, drag and drop to copy the logs and the database to the original location.
6. To use the **ESEUTIL** utility to check the restore, go to the command line and enter the following command:

   `eseutil -mh database.edb`
7. Go to the **Exchange System Manager** window.
8. In the Exchange System Manager window, expand the Servers folder.
9. Right click to select the required Exchange server and storage group; then, click **Mailbox Store** > **Mount**.

Restoring data from Microsoft Exchange 2007 Cluster Continuous Replication

About this task

To restore data for Microsoft Exchange 2007 Cluster Continuous Replication (CCR), complete the following steps:

Procedure

1. Unmount the target database.
2. Suspend a copy of the database storage group.
3. For both nodes, delete all of the files in the storage group folders.

4. Use FastBack Mount or instant restore to restore all the storage group files from a snapshot to the active node.
5. Mount the restored database.
6. On the passive node, run an update storage group copy on the storage group.

Results

The database is operational and replication is working.

Restoring data from Microsoft Exchange 2010 Database Availability Group

About this task

To restore data for a Microsoft Exchange 2010 Database Availability Group (DAG), complete the following steps:

Procedure

1. Dismount the target database.
2. Suspend a copy of the database.
3. Use FastBack Mount or instant restore to restore database from a snapshot to a DAG member.
4. Mount the restored database.

Results

The database is active and replication is working.

SQL backup and restore

Tivoli Storage Manager FastBack provides enhanced backup and restore capabilities for Microsoft SQL Server 2000, 2005, and 2008 Standard Edition databases and transaction logs, without compromising either data integrity or performance of online operations.

The following list details the support that is offered for Standard Editions of Microsoft SQL Server 2000, 2005, and 2008 databases and transaction logs:

* Transparent integration with the SQL server by using an SQL native API for the backup task.
* Volume Shadow Copy (VSS) service, a type of application quiescing, for SQL Server 2005 and SQL Server 2008 on Windows Server 2003 and Windows Server 2008. You cannot use a VSS quiescing application to back up utility partitions. If you need an application-aware snapshot, do not use VSS application quiescing.
* IBM application quiescing for SQL Server 2000 installed on Windows Server 2000 and Windows Server 2003.
* Back up and restore of SQL databases that are on a single volume, or are spanned over multiple volumes.
* Back up and restore of SQL databases that contain multiple data files or multiple log files.
* Back up of multiple databases simultaneously, without interruption to SQL server operation.

- Real-time restore for tables, views, and other SQL elements using FastBack Mount. You can mount virtual volume with backed up database and recover all that you need without restoring the volume to disk.
- Tivoli Storage Manager FastBack supports named instances, however, named instances are not displayed in FastBack Manager. Non-named instances are displayed in FastBack Manager.

The following points relate to Recovery Model support:
- Tivoli Storage Manager FastBack supports backup using the Simple Recovery Model. If a database is marked as Full Recovery Model, the database is backed up, but the logs are not purged.
- Named instances are not displayed in FastBack Manager.

Supported SQL versions

The following SQL versions are supported:
- Microsoft SQL Server 2000 Standard Edition - On Windows 2003.
- Microsoft SQL Server 2000 Enterprise Edition with Service Pack 2 and later - On Windows 2000 Server with Service Pack 4 or Windows 2003 Enterprise.
- Microsoft SQL Server 2005 Standard Edition (32 bit and 64 bit).
- Microsoft SQL Server 2005 Enterprise Edition (32 bit and 64 bit).
- Microsoft SQL Server 2008 Standard Edition (32 bit and 64 bit).
- Microsoft SQL Server 2008 Enterprise Edition (32 bit and 64 bit).

If both Microsoft Exchange Server and Microsoft SQL Server are concurrently installed on the same computer, you must create a dedicated policy to individually back up each server.

The following table summarizes the best practices that regard how to use the VSS service and SQL scripts on various operating systems and SQL servers:

Table 28. Using the VSS service and SQL scripts on operating systems and SQL Servers

	SQL Server 2000		SQL Server 2000		SQL Server 2000	
	Default	Named Instances	Default	Named Instances	Default	Named Instances
Windows 2000	FastBack Client Application Quiescing	XRSQL Scripts	-	-	-	-
Windows 2003	FastBack Client Application Quiescing	XRSQL Scripts	VSS service	VSS service	VSS service	VSS service
Windows 2003 64 bit	-	-	VSS service	VSS service	VSS service	VSS service
Windows 2008 64 bit	-	-	VSS service	VSS service	VSS service	VSS service

If you run the supported SQL Server 2005 software, select both log and data volumes, and select VSS application quiescing, the backup works.

If you run the supported SQL Server 2000 software, use the IBM application quiescing and back up both data and log files. If you run named instances, use scripts to back up.

Tivoli Storage Manager FastBack can also back up the SQL Server in a Microsoft Cluster Server environment. The FastBack Client must be installed on all nodes in the cluster. The following table provides you with an environment support matrix:

Table 29. Environment support matrix for SQL Servers in Cluster Server environments

	Windows Server 2003 Cluster Server (32 bit)	**Windows Server 2003 Cluster Server (64 bit)**	**Windows Server 2008 Cluster Server (64 bit)**	**Veritas Cluster Server / Windows Server 2003 (32 bit)**	**Veritas Cluster Server / Windows Server 2003 (64 bit)**
Microsoft SQL Server 2000	Yes	SQL 2000 only available on Itanium processors	No	No	No
Microsoft SQL Server 2005 (32 bit)	Yes	No	Yes	No	No
Microsoft SQL Server 2005 (64 bit)	No	Yes	Yes	No	No
Microsoft SQL Server 2008 (32 bit)	Yes	No	No	No	No
Microsoft SQL Server 2008 (64 bit)	No	No	No	No	No

Both snapshot and CDP are supported for the SQL Server, both named and non-named instances.

Tivoli Storage Manager FastBack SQL back up
About this task

SQL databases are based on data and log files. Back up of log files without data files is not supported; both data and log files must be backed up for successful restore. FastBack Server backs up entire volumes that contain data and log files, and restores either a volume, single folder or file, or single table by using FastBack Mount.

Creating an SQL snapshot policy
About this task

You can use the Simple Snapshot wizard to create an SQL snapshot policy and change policy parameters.

Click the wizard icon, [icon] . Click **Simple Snapshot Wizard**.

Note: If two different job schedules that run on the same SQL volumes, are scheduled for the same time, the full backup job schedule is completed before the incremental job schedule.

Procedure

1. For consistent backup, you must select either SQL Server or each database separately. All data, including the database, on the selected volumes is backed up. Volumes corresponding to selected databases are selected automatically.

2. Type the client group name.

3. Select the job type:
   - Full forever - a full snapshot of the client group is taken each time. The `Full` option is used when only a single full image of the volume is required at a certain point, rather than continuous incremental snapshots.
   - Incremental forever - After the first full snapshot, only incremental snapshots are taken.

4. Define and select options as follows:
   - Define how often the snapshot is run in the **Run Every** field.
   - To prevent the job from being run during specific times of the day, enable and define the **Exclusion Period**.
   - For **Perform task on**, select the days that the policy is to run.

5. If appropriate, enable disaster recovery.

6. Click **Apply** to save changes.

7. Change the storage groups to be backed up by editing the client group of the same snapshot policy.

Results

If you have a volume that contains several databases and you choose only one database to back up, when you restore the volume, after the restore, only that database is consistent.

For improved performance, separate the internal, also known as system, and external, also known as user, databases to different volumes. If all of the databases are on the same volume, you must stop the SQL server to restore external databases by using `Volume Restore` or `Instant Restore`.

Editing SQL snapshot policy

Editing an SQL snapshot policy follows the same steps as creating one, see "Creating an SQL snapshot policy" on page 155.

Advanced options
Procedure

1. Click **Advanced**.

2. The default job schedule initial time is the current system time. You can change the time, in the 24-hour time format, when the job is initiated.

3. To stop running the job after a particular date, select **End by** and type the date when the job schedule stops running. To stop running the job schedule after a specified number of times, select **End After** and type the number of occurrences. You might not want this job to run during the peak usage hours of the day. To set a space of time, during which this job does not run, select **Exclusion Period** and type the **From** and **To** hours, during which the job does not run. The default value is *none* or *zero* hours.

Application Aware options (Windows only)
About this task

The global application aware parameters are inherited from the **Applications** tab (**Configuration** > **General Configuration** > **Applications**) for all the jobs. However, these parameters can be changed for each specific job.

Procedure

1. Click **Application Aware**.
2. Define the parameters as follows:

    Preserve application consistency
    Creates consistent database snapshots by using quiescing. There are two quiescing options: either the Volume Shadow Copy service or IBM application quiescing.

    You cannot use application quiescing and the VSS service at the same time. In addition, you cannot use VSS application quiescing to back up utility partitions.

    Use IBM application quiescing for supported Windows 2000 and Windows XP operating systems.

    Use VSS application quiescing for supported Windows 2003 and later operating systems. If you need an application-aware snapshot, do not use VSS application quiescing.

    To back up applications that run on supported Microsoft SQL and Microsoft Exchange servers, verify that the VSS service is supported to take snapshots of the application.

    Purge Exchange server log files
    This option might be displayed, but it does not apply to SQL.

Results

In some cases, if a database that is being backed up is spread across many volumes, the first full snapshot might not be consistent. However, the following incremental snapshots are consistent.

If IBM application quiescing is selected, the user exit-point scripts do not run, even if selected.

Tivoli Storage Manager FastBack SQL restore

With Tivoli Storage Manager FastBack, you can restore a single database or multiple databases. The databases can be internal or external databases.

One snapshot provides several ways to restore a database in SQL server with Tivoli Storage Manager FastBack:

- Volume Restore
- Mount the snapshot to a virtual volume with FastBack Mount
- Disk Restore
- instant restore

Restoring external databases
About this task

To restore an external database, complete the following steps:

Procedure
1. Disconnect all active users from the database.
2. Detach all the external databases on the target volumes.
3. In FastBack Manager, from the Snapshots Monitor tab, choose a volume to restore.
4. Right click the volume; then, click **Restore** > **Volume Restore**.
5. Select the destination volume and click **Apply**.
6. If you have additional volumes, complete the following steps:
   a. Detach all the external databases on the target volumes.
   b. From the Snapshots Monitor tab in FastBack Manager choose volume to restore.
   c. Right click the volume; then, click **Restore** > **Volume Restore**.
7. Use Enterprise Manager to attach the restored databases to SQL server. You can also use the `Attach T-SQL` command by using Query Analyzer, or batch processing by using the OSQL utility.

What to do next

If internal databases are on the target volume, instead of detaching and attaching the databases, stop and start the SQL server service.

Rebuilding the Master database
If the Master database is lost, the SQL server is unable to start. The Master database needs to be rebuilt and restored from a recent backup.

About this task

To rebuild the Master database, complete the following steps:

Procedure
1. From the SQL installation CD, copy `\x86\data` folder to your local hard disk.
2. Remove the read-only attribute on the files inside the `\x86\data` folder.
3. Go to the folder that contains the `rebuildm.exe` file, and run it. Enter the path for the files you copied.
4. Enter your server name and collation settings.
5. After `rebuildm` finishes, a confirmation message is displayed.
6. Start the SQL server service.
7. Open **Enterprise Manager** and log on to SQL server.
8. From **Enterprise Manager**, attach the selected database.
9. Using SQL backup, you must back up to a local backup device.
10. Stop the SQL server service.
11. Start the SQL server service in single user mode by using the **-c** and **-m** command line options. For example, `sqlservr.exe -c -m`

12. Using Query Analyzer, use the restore database master from backup device command. Add the *WITH REPLACE* clause to replace the new Master database with the old one from the backup. The backup device is your predefined backup device.

Restoring Model or MSDB databases
About this task

Model or MSDB databases are SQL server internal databases and need to be restored in a different way from external databases. To restore Model or MSDB databases use the following procedure:

Procedure
1. Stop SQL server service.
2. Copy the backup files into the SQL /DATA directory.

Volume restore
Volume restore can be used to restore an external database located on one volume, or that spans several volumes.

Restoring to the default location or to another location can be accomplished by using the Enterprise Manager to attach the restored databases to the SQL server. You can also use the **attach** command by using Query Analyzer, to attach it to the selected SQL Server.

The following example demonstrates the procedure:
- An SQL server has an external database that is located in volume E.
- The database was backed up using the FastBack Server and then deleted from the SQL server.
- The database was restored to the same or different location by using the FastBack Server Volume Restore.

You can use the attach methods to attach the database to the SQL server again. If the database contains less than 16 files, then use Enterprise Manager. If the database contains more than 16 files use Query Analyzer to write the **Transact-SQL** command to attach the database.

The following example shows the command:
```
CREATE DATABASE database_name
ON PRIMARY (FILENAME = 'X:\filename.mdf')
FOR ATTACH
```

Mount the snapshot to a virtual volume by using FastBack Mount
You can use FastBack Mount to mount a backup volume and attaching the database to SQL without the need to restore. As a result, you can restore a single table or any other data from a database to SQL server.

When a database is backed up, it is in the FastBack Server repository. So a virtual volume that contains the database can be mounted on any SQL server.

Note: For Windows 2003 server users, to attach the database to SQL, the volume must be mounted as read/write. Ensure that you do not select **Mount as read only** in the Add drive letter path at the beginning of the mounting process. If the read only option is selected, changes are not saved.

After the volume is mounted the database needs to be attached to the SQL server. Extract the necessary data and export it to the production SQL server.

To mount a snapshot, FastBack Mount must have access to a repository disk (through SAN or LAN). Do not write to the attached database on the mounted volume, because all changes are lost after dismounting. If you want to keep changes, copy the snapshot to another volume.

Disk Restore

Disk Restore is used in situations where system and disk level recovery is required.

Because a restore is done on disk level or volume level, all SQL databases on the source volumes are restored. When disk-level restore is done while the target operating system is running, follow the instructions described in "Restoring external databases" on page 158.

When disk restore is done, no additional actions are required because the entire system is brought back to a certain point in time.

Backing up and restoring Lotus Domino Databases

Lotus Domino does not provide a mechanism to capture consistent snapshots of Domino data volumes while the Domino server is online so the following two approaches can be used to back up Domino databases with Tivoli Storage Manager FastBack:

* To ensure a consistent backup, shut down and restart the Domino server when the snapshot consistency point was created.
* Rely on Domino crash recovery if transaction logging is employed (circular mode) and most database files on the Domino server are logged.

The following sections that follow describe the characteristics of these two approaches. The procedures described assume that the Domino data and log volumes are dedicated to the Domino server and do not contain data for other applications.

If any files not belonging to the Domino server exist on these volumes, they are in an unknown state. These files might be inconsistent when the snapshot is complete. Non Domino data cannot be placed on these volumes unless it does not matter if these files are lost or corrupted by a volume level restore.

Supported environments

Tivoli Storage Manager FastBack supports the use of procedures described in this section for the backup and restore of Domino servers in the following environments:

* Domino 6.5.5 or later
* Windows Server 2000 SP3 or later, or Windows Server 2003 SP1 or later (32-bit or 64-bit) as supported by the Domino server used

(Windows 2000 only) If the Domino Server is installed on the Windows 2000 platform, **tlist** must be installed as a prerequisite for running the FastBack script. This file is available on the Windows 2000 CD under 2000Disk\Support\Tools\ SUPPORT.CAB. If isDominoService false is set in the domino_presnapshot.cmd scripts, the Domino Server restarts if the server is running as a regular application

by default. Before backing up Domino, you need to start Domino as a regular application, and check the box if you do not want to be asked again.

For Domino servers that use DB2 as the data store rather than NSF files, both the offline and online snapshot approaches can be used for full server recovery. Individual Domino database recovery is not available.

Domino servers that use archival transaction logging are not supported by Tivoli Storage Manager FastBack.

Snapshots of an offline Domino server

The Domino server is shut down before creation of a snapshot. For this reason, a consistent backup image of all Domino databases on the server is captured by the snapshot of the data volumes.

Because Tivoli Storage Manager FastBack does volume level snapshots, each snapshot creates a new backup version of each Domino database on the data volumes included in the backup.

This type of backup enables volume level recovery in disaster situations. In addition, you can use FastBack Mount to restore individual NSF files from a snapshot image.

Tivoli Storage Manager FastBack supports offline snapshots of Domino servers that run without transaction logging or those running in circular log mode. Domino servers that run in archival log mode are not supported by Tivoli Storage Manager FastBack.

Although the transaction log is not needed to restore offline backups of NSF files, if the Domino server is employing transaction logging, the transaction log volume is to be included in the snapshot for scenarios where the full Domino server needs to be restored. In that case, restoring the log volume together with the data volumes improves the recovery time when the restored server is restarted.

Tivoli Storage Manager FastBack provides the scripts to shut down a Domino server before establishing the consistency point and then to restart it after the copy-on-write process is initiated. These scripts can be used by specifying them on the Pre and Post Processes tab when defining the backup policy for Domino servers using FastBack Manager.

Restoring an individual NSF file
About this task

To restore individual NSF files from an offline backup, with the Domino server up and running, complete the following steps:

Procedure
1. Use FastBack Mount to select the snapshot image from where the NSF file is restored and mount it to the Domino server system.
2. Use the Domino Administrator interface to take the database that you want to restore offline. After the database is offline, delete the database.
3. Use Windows Explorer to copy the desired NSF file from the snapshot volume mounted through FastBack Mount to the Domino data directory.

What to do next

The restored database can be opened and used as normal.

Restoring all databases on a Domino server
About this task

To complete a full restore of all databases on the Domino server from an offline backup, complete the following steps:

Procedure
1. Shut down the Domino server that you want to use for the restore.
2. Restore the data and transaction log volumes by using one of the following methods:
   - Use the FastBack Mount interface to complete an instant restore of the snapshot images that represent the backup version to be restored. This includes the data and transaction log volumes, if Domino transaction logging is being used.
   - Use the FastBack Manager interface to do a volume restore of the data and transaction log volumes from the wanted snapshot.
3. Restart the Domino server and use it as normal.

Restoring an individual item from an NSF file
About this task

This procedure is similar to the one used to restore an individual NSF file as it can be done with the Domino server up and running:

Procedure
1. Use FastBack Mount to select the snapshot image that contains the NSF file version from which an item is to be restored and mount it to the Domino server system.
2. Use Windows Explorer to copy the wanted NSF file from the snapshot volume, mounted through FastBack Mount to a location where it can be accessed by the user that owns the database by using a different name. For example, `dbname_copy.nsf`.
3. Use the Domino Administrator interface to disable replication for the copied database.
4. Notify the database owner that the restored database copy is available.

What to do next

The database owner can now open the database copy by using the Notes® client to copy the wanted item to the primary database. This step is to be completed by the database owner to ensure that the encrypted databases remain secure.

Snapshots relying on Domino crash recovery

When using a snapshot that relies on Domino crash recovery, no action is taken to quiesce the Domino server when the snapshot is complete.

Before you begin

Instead, the data and log volumes are snapped together while the Domino server is online. This step ensures that, at restore time, Domino crash recovery processing can be used to bring the databases to a consistent state. These databases were open when the snapshot was created. Any databases that are not logged, and that are open at the time of the backup, require fixup to be run.

Although crash recovery can be completed when Domino transaction logging is not used, the time required to run fixup against many databases makes this approach impractical. Using the transaction logging makes crash recovery feasible.

Because crash recovery processing is necessary to recover databases backed up using this approach, restore of individual NSF files from an online snapshot is cumbersome and complicated. It requires an alternate Domino server system.

About this task

To complete a full restore of all databases on the Domino server, complete the following steps:

Procedure

1. Shut down the Domino server that you want to use for the restore.
2. Restore the data and transaction log volumes by using one of the following methods:
   - Use the FastBack Mount interface to complete an instant restore of the snapshot images that represent the backup version to be restored. This instant restore is to include the data and transaction log volumes, if Domino transaction logging is being used.
   - Use the FastBack Manager interface to complete a volume restore of the data and transaction log volumes from the wanted snapshot.
3. Restart the Domino server. When the server is restarted, the Domino crash recovery processing is implemented for any necessary cleanup. The cleanup makes all databases, that were open at the time the snapshot was taken, consistent using the following tools:
   - For logged databases, the transaction log.
   - For databases that are not logged, the fixup utility.

Tips

To back up Domino servers with Tivoli Storage Manager FastBack, use the offline snapshot method. This method ensures consistent backups. In addition, you can recover an entire server and individual NSF files.

If an alternative backup and recovery solution is used for recovery of individual NSF files (for example, one that uses the Domino online backup API), the Tivoli Storage Manager FastBack online snapshot might be useful to augment that solution. Tivoli Storage Manager FastBack is to provide for much faster disaster recovery processing when a full Domino server needs to be restored.

Configuring Tivoli Storage Manager FastBack for offline backup of Domino servers

The following instructions for configuring Tivoli Storage Manager FastBack for offline backup of Domino servers assume that you created a client group and a policy for the Domino server.

About this task

The following scripts are installed in the Tivoli Storage Manager FastBack scripts directory, when the FastBack Client is installed on the Domino system that is being protected:

- (Windows only) `domino_preconpoint.cmd`
- (Windows only) `domino_presnapshot.cmd`
- (Linux only) `domino_preconpoint.sh`
- (Linux only) `domino_presnapshot.sh`

(Windows only) The default directory for the scripts is `C:\Program Files\Tivoli\TSM\FastBack\client\scripts\`.

(Linux only) The default directory for the scripts is `/opt/IBM/Tivoli/TSM/ FastBack/client/scripts`

Important: (RedHat Enterprise Linux only) In the `etc/sudoers` file, comment the following line:

```
Defaults    requiretty
```

Procedure

1. Edit the scripts to contain the correct values for the variables to meet the current environment. Each script has a variables section at the beginning. You can customize the following variables:

   NotesProgram
   > Domino product installation directory.

   Directory
   > Domino data directory.

   DominoServiceName
   > Name of the service that runs the Domino server instance.

   isDominoService
   > Flag if Domino server runs as a service. The possible values, not case-sensitive, are *true* and *false*.

   doLogging
   > Flag to log the script output. The possible values, not case- sensitive, are *true*, to create a log, and *false*, to not create a log.

   LogDir The absolute path of the log directory. For all Windows operating systems, the following path is the default installation directory: `C:\Users\All Users\Tivoli\TSM\FastBack`

   Note: The *LogDir* directory must exist. The log filename is generated with this pattern: `{script name}_{date}_{time}.log`

2. Open FastBack Manager by selecting **Start** > **Programs** > **Tivoli Storage Manager** > **FastBack** > **FastBack Manager**.

3. Log on to the console with the correct user name and password. The default user name is *admin*. The default password is *admin123*.

4. (Linux only) Verify that Domino session is running. From the command prompt, you can use the following command to determine whether a Domino server session is running:

```
ps -ef | grep notes
```

If nothing is returned, no Domino server session is running. To start a Domino server in a console, enter the following command:

```
/opt/ibm/lotus/bin/server
```

A lot of information is displayed. Click **Enter** to display a clear console session.

5. Use the following procedure to configure the Domino backup. Each policy comprises one or more selected client groups and one job schedule.

   a. Under Client Groups, select the Domino application.

   b. Select the volumes allocated to Domino data and logs.

   c. Click **Apply**.

6. Use the following procedure to edit the Domino policy settings and set the scripts for Pre and Post Processes:

   a. Expand the Policies node, and select the Domino Policy.

   b. Click **Pre and Post Processes**.

   c. Select **Pre consistency-point**. For the script, type one of the following file names:

      - (Windows only) `domino_preconpoint.cmd`
      - (Linux only) `domino_preconpoint.sh`

   d. Select **Pre Snapshot**. For the script, type one of the following file names:

      - (Windows only) `domino_presnapshot.cmd`
      - (Linux only) `domino_presnapshot.sh`

   e. Do not select **Post Snapshot**. There is no need to implement any action through using the post snapshot script.

   f. Click **Apply**.

What to do next

You might also need to change the timeout interval in the **Cancel process if it is not completed within x minutes** field. The default value of *10* minutes is adequate for most environments, but if a normal shutdown of the Domino server takes more than 8 minutes, then this value is to be increased to 2 minutes greater than the time required for a normal shutdown of the server.

(Linux only) If you mount the backup snapshot as default (read-only) and copy to the Domino server data, the server posts the following message:

```
Hardware/OS error (Cannot write or create file (file or
disk is read-only)) writing to database (/volume1/log.nsf)

Cannot write to log file: Cannot write or create file (file
or disk is read-only)
```

After you restore Domino data and receive this error message, run the following command to successfully restore Domino data:

```
chown -R notes:users /<restored_volume_mount_name>
```

where *notes* is the owner of the Domino system, *users* is the *notes* group, and *<restored_volume_mount_name>* is the Domino data path.

Considerations and usage notes for Domino backup scripts

Use the following list of considerations and usage notes for Domino backup scripts:

1. You must edit the scripts to specify the correct values for the variables used inside the script. These values are to meet the system environment. The variables section is at the beginning of the script.

2. If a clean shutdown does not complete within the timeout period, Domino has a server shutdown timeout feature that does an **nsd -kill**. You must ensure that this timeout value is greater than the Tivoli Storage Manager FastBack timeout value on the Pre or Post Processes tab for the Domino backup policy.

   To ensure a consistent backup, the server must be shut down cleanly, rather than with the **nsd –kill** function. By ensuring that the Domino server shutdown timeout value is greater than the Tivoli Storage Manager FastBack timeout value, you avoid capturing a backup with potentially inconsistent data.

3. (Windows only) If the Domino server is down when the backup process is started, the scripts you run check if the server was shut down cleanly or if it failed. The backup process continues only if it was a clean shutdown.

4. The scripts provided restart the Domino server only if the server is shut down by the scripts. For Windows systems, if the server is already down when the backup starts, the server is not restarted by the scripts after the backup. For Linux systems, before backing up Domino, a Domino server console is to be opened and you are to know what Domino session is running.

5. (Windows only) Running the scripts requires administrative privileges because the scripts start and stop system services and processes. The scripts are to run as system administrator.

6. (Linux only) Running the scripts requires administrative privileges because the scripts start and stop system services and processes. When you run the scripts, verify that the logon credentials match the credential of the user that owns the Domino server.

   The Domino data is owned by the *notes* user. This *notes* user is the user you create when installing Domino. The FastBack Server backs up the Domino data as a root user. Restore the Domino data and change the data rights from root to *notes*.

7. If the *doLogging* variable is set to *TRUE*, a trace log is created in the log directory. The trace log filename has the following pattern: `{script name}_{date}_{time}.log`.

8. The log directory can be customized by the *logDir* variable. For all Windows operating systems, the following path is the default installation directory: `C:\Users\All Users\Tivoli\TSM\FastBack`

9. If the *doLogging* variable is set to *FALSE*, no log is created.

10. If a script runs without a problem, the return code is *0*. If a problem occurs when the scripts run, a non-zero value is returned. For example:
    - If the `domino_presnapshot` script runs as a standard user (a domain user) without administrative permissions, and attempts to start Domino server as a service, the script fails to start the Domino server, and returns the code *2*. In this case, an error message is displayed in the log and on the user interface.

- If the `domino_preconpoint` script runs as a standard user (domain user) without administrative permissions, the script fails to stop the Domino server and returns the code *128*.

11. The pre snapshot script runs asynchronously. The script runs the volume backup process to start when the server is restarting.

Backing up and restoring DB2 UDB databases

Tivoli Storage Manager FastBack supports snapshots of online DB2 UDB databases. The restore procedure and the choice of available recovery points differ depending on whether archive or circular logging is used. The snapshot procedure is the same.

Scripts are provided with Tivoli Storage Manager FastBack to momentarily suspend writes to the database, to initiate the snapshot, and then resume writes after the Tivoli Storage Manager FastBack snapshot copy-on-write mechanism is initiated.

When archive logging is used, restored databases can be rolled forward to any point in time up to the end of the current logs. This technique provides maximum flexibility for choosing a recovery point and provides recovery with no data loss. Native DB2 facilities or legacy backup solutions can be used to archive the log. Tivoli Storage Manager FastBack does not provide support for archiving the transaction log.

When circular logging is used for a database, DB2 recovers only to the time a backup was completed so the number of recovery points available is limited by the number of available snapshot versions.

You should not use Continuous Data Protection with DB2 databases because recovery to an arbitrary point-in-time using continuous data protection does not guarantee a consistent database. Recovery to a specified point it time with consistency can be accomplished by restoring a snapshot and applying transactions from the transaction log to get to the desired point.

To back up DB2 databases with Tivoli Storage Manager FastBack, use the provided scripts by specifying them on the Pre or Post Processes tab when defining the backup policy for DB2 databases through FastBack Manager.

Supported environments

Tivoli Storage Manager FastBack supports the use of procedures described in this section for the backup and restore of DB2 UDB databases in the following environments:
- DB2 UDB V8 or later
- Windows Server 2000 SP3 or later, as supported by the DB2 UDB version used
- Windows Server 2003 SP1 or later (32-bit or 64-bit) as supported by the DB2 UDB version used

Best practices

The following practices apply to backing up and restoring DB2 UDB databases:
- Use separate volumes for data and logs. These volumes are to be different than the volume where you installed the DB2 server. If two databases or more share at least one automatic storage path, the split mirror operation for one of these

databases might affect more than one database. This situation causes I/O problems for the databases that were not intended to be split.

- The procedures described in the following sections assume that the DB2 data and log volumes are dedicated to the DB2 database that is being backed up and do not contain data for other applications or other DB2 databases. If any files not belonging to the DB2 database exist on these volumes, they are in an unknown state and might be inconsistent when the snapshot is complete. No non-DB2 data files be placed on these volumes unless it is acceptable for these files to be lost or corrupted by a volume level restore.

- Ensure that the snapshot contains all containers and directories that comprise the database, including the volume directory. To gather this information, reference the **DBPATHS** administrative view, which shows all the files and directories of the database that need to be included in the snapshot.

- Both the log and data volumes are to be included in the snapshot set for each database backup.

- In a partitioned database environment, it is not necessary to suspend writes on all partitions simultaneously. You can use the Tivoli Storage Manager FastBack DB2 scripts to back up each partition independently while archive logging is used. In that case, restore of an individual partition requires roll forward recovery to be done to the end of logs.

- Snapshots completed by Tivoli Storage Manager FastBack do not interfere with traditional backups completed that used the DB2 backup command and are not recorded in the DB2 backup history.

Restoring a database by using archive logging
About this task

When a failure occurs on the primary system, a restore from backup is necessary. Follow these steps to implement the recovery:

Procedure

1. Run the following command to stop the primary database instance: `db2stop`
2. Restore the data volumes by using one of the following procedures:
   - Use FastBack Mount to complete an instant restore of the snapshot images that represent the backup version. This restore is to include the data volumes taken after roll forward recovery. The most current log files are required.
   - Use FastBack Manager to complete a volume restore of the data volumes only from the wanted snapshot. Do not restore log volumes.
3. Run the following command to start the primary database instance: `db2start`
4. Run the following command to initialize the restore database: `db2inidb <alias name> as mirror`
5. Roll the primary database forward to the end of the logs, or to a point-in-time and stop. For example,

   `db2 rollforward db <alias name> to end of logs and stop`

What to do next

The restored database can now be opened and used as normal.

The following best practices apply:

1. In a partitioned database environment, if a subset of the database partitions is restored, the restored partitions must be rolled forward to the end of logs.

2. In a partitioned database environment, the **db2inidb** command must be run on every restored partition before the snapshot image from any of the partitions can be used. The tool can be run on all partitions simultaneously by using the **db2_all** command.

3. Do not issue the **db2 connect to** *<database>* command before issuing the **db2inidb** *<database>* **as mirror** command. Attempting to connect to a restored snapshot image before initializing it, erases the log files needed during roll forward recovery.

Restoring a database by using circular logging
About this task

When a failure occurs on the primary system, a restore from backup is necessary. Follow these steps to implement the recovery:

Procedure
1. Run the following command to stop the primary database instance: db2stop
2. Restore the data volumes by using either of the following methods:
   a. Use FastBack Mount to complete an instant restore of the snapshot images that represent the backup version to be restored. This restore is to include the data volumes and log volumes after roll forward recovery cannot be finished.
   b. Use FastBack Manager to complete a volume restore of the data and log volumes from the wanted snapshot.
3. Run the following command to start the primary database instance: db2start
4. Run the following command to initialize the restore database:

   db2inidb *<alias name>* as snapshot

What to do next

The restored database can now be opened and used as normal.

The following best practice applies: In a partitioned database environment, the **db2inidb** command must be run on every partition before the snapshot image from any of the partitions can be used. The tool can be run on all partitions simultaneously by using the **db2_all** command.

Configuring Tivoli Storage Manager FastBack for online backup of DB2 UDB
About this task

The procedure described assumes that the following tasks are completed:
- Installed the FastBack Client on the DB2 system.
- Created a client group for the DB2 database.
- Created a backup policy for the DB2 database.

(Windows only) The default directory for the scripts is C:\Program Files\Tivoli\TSM\FastBack\client\scripts\.

(Linux only) The default directory for the scripts is /opt/IBM/Tivoli/TSM/ FastBack/client/scripts

Procedure

1. Edit the `db2_executeSQL` script to contain the correct values for the following variables to meet the current environment. The variables section is marked at the beginning of the script.

   dbuser User ID that has the following authorities: *sysadm*, *sysctrl*, or *sysmaint*.

   dbpass Password for the *dbuser* user ID.

   dbinst DB2 instance name that runs the database.

   dbname
   > Database alias to back up.

2. If you do not want to accept the default logging parameter values, edit the `db2_preconpoint`, `db2_presnapshot`, and `db2_postsnapshot` scripts to change the following two variables.

   doLogging
   > Flag to create a trace log. The possible values: *TRUE* and *FALSE*. The default value is *TRUE*.

   logDir The absolute path of the log directory. For all Windows operating systems, the default path is `C:\%ALLUSERSPROFILE%\Application Data\Tivoli\TSM\FastBack\DB2Agent`. For all Linux operating systems, the default path is `/opt/IBM/Tivoli/TSM/FastBack/DB2agent`

   Note: The log file names are generated using this pattern: `{script name}_{date}_{time}.log`

3. Open FastBack Manager and logon by using the correct user name and password.

4. Use the following procedure to configure the DB2 backup. Each policy comprises one or more selected client groups and one job schedule:

   a. Under the Client Groups definition, select the volumes allocated to the DB2 data and logs.

   b. Click **Apply**.

   c. Edit the DB2 policy settings and set the scripts for Pre and Post Processes:

      1) Expand the Policies node, and select the DB2 policy.

      2) Click **Pre and Post Processes**.

      3) Select **Pre consistency-point**. For the script, type one of the following file names:
         - (Windows only) `db2_preconpoint.cmd`
         - (Linux only) `db2_preconpoint.sh`

      4) Select **Pre Snapshot**. For the script, type one of the following file names:
         - (Windows only) `db2_presnapshot.cmd`
         - (Linux only) `db2_presnapshot.sh`

      5) Select **Post Snapshot**. For the script, type one of the following file names:
         - (Windows only) `db2_postsnapshot.cmd`
         - (Linux only) `db2_postsnapshot.sh`

      6) Click **Apply**.

Recovering operating system partitions by using Disk Restore

To use Disk Restore for the recovery of operating system partitions, go to FastBack Manager.

Click the Recovery tab and select **Disk Restore**. Using this option you can create a new disk from snapshots of several volumes. You can recover entire systems to a comparable server, to a new server with different hardware, or to a virtual machine (VMware or Microsoft Virtual Server).

When completing a disk restore to a Hyper-V virtual machine, use the following list of tips:

- The target virtual machine for the disk recovery must have a legacy network adapter. You can add a legacy network adapter to the virtual machine by going to the Hyper-V Manager, clicking **Settings** for the virtual machine, and then clicking **Add Hardware** > **Legacy Network Adapter**.
- To have the mouse available on the Hyper-V virtual machine, install *Hyper-V Manager*. Hyper-V Manager requires the Microsoft Windows Vista, Service Pack 1, or Microsoft Windows Server 2008.
- The boot partition must be on a virtual IDE disk. Hyper-V cannot boot from a SCSI disk.

A disk restore does not provide the same disk partitioning as existed on the original disk. A disk restore provides only the requested volumes and the valid data available on those volumes. A partition becomes an extended partition beginning with the fourth partition.

Chapter 7. Maintaining

This section describes the tasks you can complete to maintain the Tivoli Storage Manager FastBack operations that you configured and use.

Server status

If the FastBack Server is working without error, status is reported as OK.

If the server is not working correct, the following list identifies some possible system errors:

- The remaining repository space exceeds the defined threshold. The threshold is defined by using the Maintenance tab.
- An unprotected or disconnected FastBack Client is identified.
- The FastBack Server is down with one of the following errors reported:
  - Limited mode: Limited mode is often caused by a repository that cannot be accessed or the system finds corrupted files on one of the repositories.
  - Fatal error: Notification initiated by server.
  - Not responding: Notification initiated by the FastBack Watchdog.

Monitoring events and snapshots

You can monitor the status of events and snapshots.

Viewing events

It is important to review the events of the last 24 hours daily. Tivoli Storage Manager FastBack provides several means for viewing system and job-related events. In addition, Client and Server events can be viewed on the corresponding Client and Server computers through the Windows Event Viewer.

Three types of events that are identified by different colors, are provided:

- White - informational events.
- Yellow - warnings events.
- Red - alert events.

Viewing FastBack Manager systems events
In the FastBack Manager tree, click FastBack Server log. The Event Viewer is displayed.

Viewing job-related events
In the **Snapshots Monitor** tab, right-click the snapshot you want and select **Events.** The events related to that snapshot are displayed. Click **OK** to close the dialog.

Viewing FastBack Client and FastBack Server events
Events specific to the FastBack Client or the FastBack Server can be displayed on the computer on which they are installed.

On the Windows Server 2003 system where you want to view events, right-click **My Computer**; then, click **Manage**. In the window, click **Events Viewer** > **Application**. Some information for each event is displayed.

Right-click the selected FastBack Client or FastBack Server event; then, click **Properties**.

Monitoring snapshots

The Snapshots Monitor view in FastBack Manager is used to display the status of snapshots, including information about each snapshot and restore activity. You can view the monitoring information by clicking the **Snapshots Monitor** tab.

The Snapshots Monitor view has two panes. The right pane displays the snapshot information and the left pane provides filters for selecting the snapshots that are displayed.

Additional information about each snapshot is available by right-clicking any snapshot in the display and clicking either **Events** or **Snapshot Properties**. Clicking **Events** provides snapshot progress information. Clicking **Snapshot Properties** provides information related to snapshot identification.

The user can change the display by filtering snapshots according to various criteria, such as start time, state, snapshot duration, and size.

You can restore a snapshot by right-clicking a selected snapshot and choosing the wanted restore option.

Snapshots Monitor tab

In the Snapshots Monitor tab, each volume snapshot is assigned a line. For example, if a Client Group consists of four volumes, four lines are displayed. Each line displays data about a snapshot for each volume.

By default, snapshots are displayed according to their start time, with the most recent snapshot as the first entry in the snapshot list. However, by clicking any of the column headers, the display can be sorted according to any other snapshot element. These elements include volume, type, job schedule, and other elements. You can also click-and-drag the columns to change the column order.

Clicking the sorting column header again changes the sorting direction.

The Backup Integrity level column displays one of two levels:

Consistent
> The file system is updated and synchronized. The system might require application-level recovery after restore.

Committed
> The snapshot data is consistent at application level and does not require recovery.

Each snapshot has an icon that displays its present status. The expired snapshots are represented by gray icons.

Table 30. Snapshots Monitor icons

Snapshots Monitor icons	Description
	Initializing or running snapshot.
	Continuous Data Protection Snapshot is running.
	Snapshot completed successfully.
	Continuous Data Protection Snapshot completed successfully.
	Successful snapshots whose retention time is expired.
	Continuous Data Protection process is terminated, but some Continuous Data Protection data is available.
	Aborted snapshots.
	Aborted snapshots whose retention time expired.

Filtering the snapshots

The display can be filtered according to relevant criteria. Any combination of criteria can be applied simultaneously:

- State (initializing, running, aborting, aborted)
- Date (last day, last two days, last week, two weeks, month)
- Selected volumes or client groups
- Job Schedule
- Selected Policies

Note: To refresh the monitor display at any moment, click **Filter/Refresh**.

Filtering the display

From the Snapshots Monitor tab, select the options of the filters and the filter options that you want. After you select a filter, the corresponding parameters are enabled and can be defined. For example, when Date is selected, the parameters *Last 24 hours*, *Last 48 hours*, *Last week*, *Last 2 weeks*, and *Last month* are available.

To apply the filtering process, click **Filter/Refresh**. Only snapshots that match all the selected criteria are displayed.

To clear the filters and reset the display, click **Show All**. The full, unfiltered list is displayed. In the Volume filter, only non-expandable items can be selected.

Viewing snapshot properties

Basic property information is provided along with each snapshot in the Snapshots Monitor tab. A summary of these properties and additional information can be viewed by right-clicking the snapshot in the Snapshots Monitor view and selecting **Snapshot Properties**.

The following information is provided for each snapshot:

- Snapshot ID - Unique identifier for the snapshot.
- Job Schedule Name - Snapshot schedule name.
- Policy Name - Snapshot policy name.
- Type of snapshot - Incremental, full, or checkpoint.
- Volume - Snapshot volume.
- State - Snapshot status (completed, running, aborted).
- Start time of the snapshot.
- End time of the snapshot.
- Size - Snapshot size.
- Rate - Rate (in MB/sec) at which the snapshot is taken.
- Data type - Snapshot source (SQL, Exchange), if any (default file system).
- Total Continuous Data Protection (CDP) data size - The size of the Continuous Data Protection data.
- Performed Quiesce Before Backup - Services stopped before backup.
- Purged Exchange Logs - Exchange log files deleted after backup.
- Performed VSS Flush - All applications supporting the VSS framework were brought to a consistent state. The file system was also brought to a consistent state.
- Content aware - If checked, the snapshot is performed on used disk space only. Unused disk space is not snapped.
- Enable DR - This snapshot is replicated to a remote location.

Viewing the event log for a specific snapshot

In the Snapshots Monitor view, right-click the snapshot and then click **Events**. The Event Log displays the start and end time of the job, whether it completed successfully, and any unusual events that occurred during the job.

Viewing pending snapshots

You can view a list of pending snapshots from FastBack Manager.

In FastBack Manager, select the **Configuration** tab. In the tree, select **Pending Jobs**. A list is displayed. The list contains the next 50 pending snapshots. The list includes the time that the snapshot is scheduled to run, the volumes to be snapped, and the job schedule defined for the snapshot.

Optimizing disk access

You can run an optimization test to determine the disk access parameters required by the system to provide optimum disk performance.

The test takes about 3 minutes per disk and only one test can run at a time. This optimization test is available for SAN disks. In addition, disk access optimization is only available for disks that are visible from the FastBack Server.

To run the optimization test, right-click the disk, click **Optimize Disk Access**. A message is displayed. Respond to the message. You can then view the results of the test in the Properties window for the disk. Select **Storage Pool**. Right-click the disk; then, click **Properties**.

Important: If you choose a dynamic disk that is mirrored, spanned, or striped by the Windows Disk Management applet, you can corrupt the data in the repository.

Cleanup

The FastBack Server snapshot repository is a disk-based solution. The repository disk space is limited. Tivoli Storage Manager FastBack uses several mechanisms to optimize the use of repository space, and to automate the process of disk cleanup. During the disk cleanup, obsolete repository data is deleted.

Cleanup processes require considerable resources. It is best to schedule and run clean up tasks during a time of day and week when snapshots are not scheduled. Running the cleanup during off-peak times reduces the risk of overload to bandwidth and FastBack Server activity.

You can schedule and run cleanup tasks when snapshots are running. The cleanup tasks use a locking mechanism to ensure consistency. Before any cleanup task runs, the cleanup process verifies that a snapshot chain is not locked. A snapshot chain is a full snapshot and the corresponding incremental snapshots of the same volume and policy combination.

If a chain is locked the cleanup process runs on the next chain that is not locked and scheduled for cleanup. A chain can be locked when a volume is mounted, or when a snapshot or instant restore is running. When a chain is unlocked and available, the cleanup process can run. When the cleanup process starts, the cleanup process locks the snapshot chain.

During the cleanup process, FastBack Server detects snapshots that are potentially corrupted. When FastBack Server detects a potentially corrupted file, a warning message is displayed and a message is written to the FastBack Server log. During the next scheduled snapshot of the volume a job is run to repair the snapshot. You must not use a potentially corrupted snapshot. If a problem occurs and you need the data before the repair job for the snapshot completes, complete the following steps:

1. Run the file system check tool. You can look at the operating system documentation for more help in completing this step.
2. Run the application consistency check tool. You can look at the operating system documentation for more help in completing this step.

Note: After the repair snapshot is completed, snapshots from that point onward are good and can be used.

Generations

When a snapshot is created, it is tagged with a number that is referred to as a *generation*. During disk cleanup, generations are a parameter used by Tivoli Storage Manager FastBack for disk cleanup.

You can set the number of snapshot generations that are saved. This number of snapshots is available for restore tasks. Older snapshots, beyond the number of generations you set, are deleted during the cleanup process. For example, you can setup snapshot occurrence to once a day, and the number of snapshot generations to 14. This means that all snapshots performed in the preceding 14 days are available for restore tasks. Snapshots older than 14 days are deleted during the cleanup process.

When you use FastBack Reporting to run and view reports, the reports include data about snapshots stored in the repository. The repository can include snapshots that are marked for deletion because the snapshots exceed the number of

generations to save threshold. These snapshots cannot be viewed from the Snapshots Monitor tab, but they are stored in the repository until the cleanup process runs and deletes the snapshot. When you run a report, all snapshots, including those that are marked for cleanup because they exceed the number of generations to save threshold, are included in the report.

In the **Snapshots Monitor** tab, the oldest of the available generations is identified, by number. The number is surrounded by bracket characters, for example, *[14]*. This number indicates the total size of data from all previous snapshots that are not visible or accessible, but reside in the repository at that moment. The size of this information can grow and exceed the size of the backed up volume. The predefined cleanup frequency affects this size.

Tip: Set the number of generations to exceed the actual number that are retained. If the number of generations is set too low, snapshots that exceed the generation value are placed in the cleanup queue during the restore operation. As a result, you cannot view that the restoring task is still running in the Snapshot Monitor.

The number of generations is defined per policy. To set the number of generations, complete the following steps:
1. Select a policy to edit.
2. Enter the number of generations in the **Number of generations** field.
3. Click **Apply**.

When creating a new policy, you define the number of generations when using the Advanced Policy Wizard.

Cleanup configuration

Setting the cleanup parameters can affect disaster recovery. When more cleanup processes are running, there is more traffic for disaster recovery. Use the cleanup level parameter to balance the time and effort of the cleanup process with the amount of data that needs cleanup.

About this task

The following list identifies the cleanup parameters:
- Cleanup scope, schedule, and occurrence are set under the **General Configuration** > **Maintenance** > **Cleanup** tab. These parameters apply to all Tivoli Storage Manager FastBack policies. You can override the parameters by editing parameters in the Policy Cleanup tab. For additional information, go to section "Policy cleanup" on page 112.
- The number of generations to be retained is a parameter that is set for each policy.
- If disaster recovery is used, there is an additional setup related to disaster recovery optimization. This setup applies to all policies handled by Tivoli Storage Manager FastBack.

Defining cleanup parameters
Cleanup requires considerable resources. Schedule and run cleanup tasks during a time of day and week when few snapshots are scheduled. Running the cleanup during off-peak times reduces the risk of overload to bandwidth and FastBack Server activity.

About this task

To define cleanup parameters, complete the following steps:

Procedure

1. In the FastBack Manager Configuration pane, choose Generation Configuration and select the **Maintenance** > **Cleanup** tab.

2. Select one of the following cleanup settings:

   Maximal Disk Cleanup
   If you do intend to replicate snapshots to a FastBack DR Hub Server server, this option is not to be selected. Selecting this option implies that a large amount of data is transferred. Transferring a large amount of data to FastBack DR Hub Server server can overload bandwidth and FastBack Server activity.

   High Disk Cleanup
   This option also requires much bandwidth, but, in general, can be used when replicating snapshots to a FastBack DR Hub Server server.

   Low Disk Cleanup
   Less bandwidth is required. This option can be used when replicating snapshots to a FastBack DR Hub Server server.

   Minimal Disk Cleanup
   This option affects bandwidth the least because less data is transferred. This option can be used when replicating snapshots to a FastBack DR Hub Server server.

3. Click **Apply**.

4. In the Repository usage alert section, you can adjust when an alert is sent. An alert is sent when repository available space is less than a specific limit. The limit for available repository space is defined by a percentage. You can type a number between *0* and *100*.

5. Click **Apply**.

6. Click **Cleanup Scheduler**.

7. Type the job schedule name. For example, this schedule is being defined for cleanup so you can name the schedule *Cleanup*.

8. Set the parameters for the cleanup schedule. Remember that cleanup requires considerable resources. Schedule and run cleanup tasks during a time of day and week when few snapshots are scheduled. Running the cleanup during off-peak times reduces the risk of overload to bandwidth and FastBack Server activity. To reduce the effect of cleanup to other operations, schedule cleanup less frequently, down to one time per week.

9. Click **Apply**.

10. Click **Advanced**. The Advanced window provides you with extra configuration options for the Cleanup Scheduler.

11. Specify the time of day in which you want the cleanup to take place, and configure cleanup jobs. Configure the parameters and click **OK**.

Immediate cleanup operations

You can request that a cleanup starts immediately, or, after a cleanup starts, you can cancel the cleanup.

To start a cleanup, complete the following steps:

1. Start FastBack Manager.

2. From the Configuration tab, select General Configuration.

3. In the work area, select the Maintenance tab.

4. In the Cleanup section, click **Run now**. **Run now** is only available when no cleanup process is running.

When a cleanup process is running, there is an indicator for the process in the FastBack Manager toolbar. The hover help for the icon indicates the progress of the cleanup process.

To cancel a cleanup process, complete the following steps:

1. Start FastBack Manager.

2. From the Configuration tab, select General Configuration.

3. In the work area, select the Maintenance tab.

4. In the Cleanup section, click **Cancel run**. **Cancel run** cancels the current cleanup process. The cleanup is not instantly cancelled. The cleanup is cancelled after the current chain cleanup is complete.

The cleanup process resumes according to the cleanup schedule.

Manual repository cleanup options

Tivoli Storage Manager FastBack offers several repository cleanup options. You can use these options to save repository space, and to ease the automated cleanup process.

Snapshot chains are series of snapshots of the same volume in the same policy. They can be manually removed by right-clicking on a snapshot in the Snapshots Monitor tab, click **Erase**, and selecting one of the following three options:

Previous snapshots in this chain
> Select this option to erase all snapshots in the chain of the selected snapshot that are older than the selected snapshot. The selected snapshot is not erased.
>
> This option is only available if you select a full snapshot. If this option is not enabled and you want to remove all older snapshots in a chain, complete a full snapshot.

This snapshot and newer ones in this chain
> Select this option to remove a specific snapshot and all newer snapshots in the same chain. A scenario for using this option is when classified information is included a snapshot, but the information needs to be hidden and removed.
>
> Removing all newer snapshots causes the next snapshot on the chain to be an incremental delta block snapshot instead of an incremental snapshot. For more information about the types of snapshots, see "Setting up snapshot policies" on page 106.

All snapshots in this chain
> Select this option to erase the selected snapshot and all of the snapshots in the chain. After you select this option, a message is displayed that explains the next snapshot is going to be full snapshot.

After selecting an option, a confirmation message is displayed. The message includes a list with the snapshots to be removed. Click **Yes** to erase or click **No** to cancel.

A snapshot that is currently being restored by instant restore is not deleted from the repository by the cleanup process until the instant restore process is complete. A snapshot that is mounted by FastBack Mount is not be deleted until it has been released from all mount processes. If an attempt is made to delete snapshots from a chain that is being used by FastBack Mount or the instant restore process, an error message is displayed.

Automatic disk cleanup process overview

When you run an automatic disk cleanup process, only one cleanup operation runs at a time.

After an automatic disk cleanup process starts, Erase Chain and Remove older snapshot processes cannot be stopped. You can run a snapshot concurrently with a cleanup job.

Extra repository space is required to complete cleanup jobs. In general, the amount of free space in the repository disk must be equal or greater than the full snapshot size.

Error recovery: Setting the number of retries

Sometimes a snapshot attempt fails. This failure can be caused by events such as a momentary overload on system resources, a SAN disconnection, or a FastBack Client disconnection (for example, for DAS backup).

About this task

Tivoli Storage Manager FastBack can be configured to reattempt a new snapshot automatically.

You can set the number of repeated attempts and the delay between attempts. If, after the number of defined attempts, the snapshot is not performed successfully, a failed job notification is sent for the next time frame. The next attempt is made according to the schedule.

Procedure

1. Expand **General Configuration**, and, in the main window, select the **Retries** tab.
2. Define the following parameters under Failed Job Recovery policy:

   Repeated attempts
   Enter the number of repeated attempts to take a failed snapshot and click **Apply**. If there are repeated attempts to take a snapshot, the entire policy runs. All volumes are included in the snapshot.

   Delays between attempts
   Enter the number of minutes between repeated attempts to take a snapshot and click **Apply**. For more information about the retry policy, see "Retry policy" on page 85.

Alerts and notifications

You can send alerts on specific events to a SMTP host. In addition, you can configure email alerts according to predefined parameters.

The FastBack Server calls the `ExternalNotification.bat` file each time an alert is generated. This batch file can be edited. When you edit the file, you can request that an email notification be sent when an alert is generated.

You can also use the batch file to apply various user-configured filters to the send notifications. The `ExternalNotification.bat` file is installed in the same directory as the FastBack Server. By default, this location is `C:\Program Files\Tivoli\TSM\FastBack\utilities`.

The `ExternalNotification.bat` file calls the `contain.exe` file. The `contain.exe` filters alerts based on the part of the alert quoted in the command. The default filters are included in the following code sample:

```
contain.exe "%XR_MSG%" "aborted" "The limit for repository"
 "Unable to initiate snapshot" "Failed to initiate cleanup on volume"
 "will not perform any snapshots"
If %ERRORLEVEL% EQU 0 goto SEND
contain.exe "%XR_MSG%" "The Exchange service failed to start"
 "The Exchange service failed to terminate"
 "The FastBackServer Failed to access Repository in path"
If %ERRORLEVEL% EQU 0 goto SEND
contain.exe "%XR_MSG%" "The Repository has Sanity Problem"
 "Repository Not found on initial" "The Repository in path"
 "The cleanup of snapshot" "Verification of job"
If %ERRORLEVEL% EQU 0 goto SEND
contain.exe "%XR_MSG%" "The repository is cleared"
If %ERRORLEVEL% GTR 0 goto END
```

Configurable parameters

The following parameters must be configured to enable email messages. These parameters can be configured either during installation or later.

- SMTP_SERVER - The SMTP server address (this field must be configured). Variable: SET SMTP_SERVER=smtp.server.name
- SMTP_PORT - The SMTP server port. The default is 25. Variable: SET SMTP_PORT=25
- SMTP_TO_ADDRESS - The receiver address (This field must be configured). Variable: SET SMTP_TO_ADDRESS=reciver_user@addr.com
- SMTP_FROM_ADDRESS - The sender address. (This field can be changed). Variable: SET SMTP_FROM_ADDRESS=sender_user@addr.com
- SMTP_SENDER_NAME - This value is the FastBack server machine name.

Note: The FastBack server host name is set as the default sender name (SMTP_SENDER_NAME).

Environment variables

Before FastBack Server calls this batch, it sets the following environment variables.
- *COMPUTER_NAME* - FastBack Server name.
- *XR_MSG* - The message to send.
- *XR_TYPE* - The notification type: *JOB_EVENT* or *EVENT_LOG*.
- *XR_EVENT_LEVEL* - The level of the event: *INFO, WARNING, ERROR*.
- *XS_JOB_TYPE* -The job type: *FULL, INC, DIFF, RESTORE*.
- *XS_JOB_SERVER_NAME* - Server name, also known as agent name; to be defined only in *JOB_EVENT*.
- *XS_JOB_VOLUME_NAME* - Job volume name; to be defined only in *JOB_EVENT*.

- *XS_JOB_ACTION_NAME* - Action item name; to be defined only in *JOB_EVENT*.
- *XS_JOB_START_TIME* - Job start time; to be defined only in *JOB_EVENT*.
- *XS_JOB_SNAPSHOT_SIZE* - The snapshot size.
- *XS_JOB_DB_TYPE* - The job database type: *NONE*, *ORACLE*, *EXCHANGE*, or *SQL*.

These environment variables are used later by the batch file to send the notifications. The batch uses the **FastBackSendMail** utility to send email messages.

The environment variables are the only way the script is built. The environment variables are not mandatory.

Disabling utilities

To disable **FastBackSendMail**, add the following string before the command: *REM*. This string indicates that the line of code is a remark. For example:

```
REM FastBackSendMail.exe -s %SMTP_SERVER% -p %SMTP_PORT%
 -t %SMTP_TO_ADDRESS% -f %SMTP_FROM_ADDRESS% -a
%SMTP_SUBJECT% -m %XR_BODY_FILE_NAME%
```

In this example, the FastBackSendMail script does not send any mail.

Using the `FastBackSendMail` utility

FastBackSendMail is an application that sends email. For **FastBackSendMail**, the following command options are available:

Parameter name	Description
-s	SMTP server name
-p	(Optional) SMTP port number; the default is 25
-t	To: Address
-f	From: Address
-b	(Optional) Text body of message
-h	Generate headers
-a	(Optional) Subject
-m	(Optional) File name; use the file as the body of the message
-h	Help

Configuring periodic email notification
Before you begin

You can configure the FastBack Server to send periodic email notifications. These emails notify the recipient about possible system errors, and reports about unprotected volumes:

- The remaining repository space exceeds the defined threshold. This threshold is defined in the **Maintenance** tab (see *Repository Usage Alert*).
- An unprotected or disconnected FastBack Client was detected.
- FastBack Server is down because of one of the following reasons:
    - Limited mode (server initiates notification)
    - Unrecoverable error (server initiates notification)
    - Not responding (notification initiated by the FastBack Watchdog

If the server is operating without any errors, an email message is sent with the following subject line:

```
FastBack Server Status: OK
```

About this task

You can also configure the FastBack Watchdog to send more frequent email notifications. For example, you can receive alerts about a disaster recovery failure or a problem with a snapshot chain.

To configure email notification, complete the following steps:

Procedure

1. (Optional) For more frequent email notifications, complete the following steps:
   a. Create a blank (empty) text file with the following file name:
      `FullHBReport.txt`
   b. Save this file in the FastBack Server directory. The default path to the FastBack Server follows: `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\server`
2. From the FastBack Manager, select **General Configuration**, click the **Alerts** tab.
3. Type in the recipient mail server.
4. Click **Add** and type in the email address for the receiving the alerts in the **Add Alerts Recipient** box.

   If needed, you can add more than one recipient email address. You can also send a test email to verify the email addresses are correct.
5. Specify how often you want to receive the alerts in hours in the drop-down menu in the **Alerts Frequency** section, and type in when you want the alerts to start.
6. Apply your changes.

What to do next

Tip: To verify that the mail server and addresses are correctly entered, click **Test E-mail**.

Tip: Click **Pause** to pause alerts, and select **Resume** when you want to restart alerts.

The complete batch file

```
@Echo OFF

REM This path should be modified if FastBack is not installed in the
REM default location
cd /d "%ProgramFiles%\Tivoli\TSM\FastBack\utilities"

:EMAIL_LABEL
REM SMTP_SERVER - The SMTP server address (this field must be configured).
SET SMTP_SERVER=exchange.domain.com
REM SMTP_PORT - The SMTP server port. The default is 25 (this
REM field must be configured).
SET SMTP_PORT=25
REM SMTP_TO_ADDRESS - The receiver address (this field must be configured).
SET SMTP_TO_ADDRESS=bill@domain.com
REM SMTP_FROM_ADDRESS - The sender address. (This field can be changed).
SET SMTP_FROM_ADDRESS=XpressServer@domain.com
```

```
REM * An IF command that checks if the current notification is Event
REM log. If yes, * it goes to the label EVENT_LOG_LABEL
IF /I %XR_TYPE% == EVENT_LOG goto EVENT_LOG_LABEL
SET SMTP_SUBJECT="FastBack %XR_EVENT_LEVEL% From %XR_MODULE% on %COMPUTER_NAME%."

echo FastBack Server Machine name - %COMPUTER_NAME% > %XR_BODY_FILE_NAME%
echo FastBack Client Machine name - %XS_JOB_SERVER_NAME% >> %XR_BODY_FILE_NAME%
echo Volume -  %XS_JOB_VOLUME_NAME% >> %XR_BODY_FILE_NAME%
echo Policy %XS_JOB_ACTION_NAME% >> %XR_BODY_FILE_NAME%
echo %XS_JOB_START_TIME% >> %XR_BODY_FILE_NAME%
echo ------------------------------------------- >> %XR_BODY_FILE_NAME%
echo %XR_EVENT_LEVEL%: %XR_MSGID% %XR_MSG% >>%XR_BODY_FILE_NAME%

goto SEND_MAIL_LABEL

:EVENT_LOG_LABEL
SET SMTP_SUBJECT="FastBack %XR_EVENT_LEVEL% From %XR_MODULE% on  %COMPUTER_NAME%"
echo %XR_EVENT_LEVEL%: %XR_MSGID% %XR_MSG% > %XR_BODY_FILE_NAME%
goto SEND_MAIL_LABEL

:SEND_MAIL_LABEL

..\common\contain.exe "%XR_MSG%" "aborted" "The limit for repository"
 "Unable to initiate snapshot" "Failed to initiate cleanup on volume"
 "will not perform any snapshots"
If %ERRORLEVEL% EQU 0 goto SEND
..\common\contain.exe "%XR_MSG%" "The Exchange service failed to start"
 "The Exchange service failed to terminate"
 "The FastBackServer Failed to access Repository in path"
If %ERRORLEVEL% EQU 0 goto SEND
..\common\contain.exe "%XR_MSG%" "The Repository has Sanity Problem"
 "Repository Not found on initial" "The Repository in path"
 "The cleanup of snapshot" "Verification of job"
If %ERRORLEVEL% EQU 0 goto SEND
..\common\contain.exe "%XR_MSG%" "The repository is cleared"
If %ERRORLEVEL% GTR 0 goto END

:SEND
FastBackSendMail.exe -s %SMTP_SERVER% -p %SMTP_PORT% -t %SMTP_TO_ADDRESS%
 -f %SMTP_FROM_ADDRESS% -a %SMTP_SUBJECT% -m %XR_BODY_FILE_NAME%


:end
del %XR_BODY_FILE_NAME%
```

Limited mode

About this task

The FastBack Server enters limited mode in one of the following situations:

- One of the repository locations cannot be accessed. For example, no network
  access to a network folder, or a volume drive letter changed. To solve this
  problem, complete the following steps:

  1. Go to **Configuration** > **General Configuration** > **Storage pool** > **Repository Pool**.
  2. The line of the repository that triggered limited mode is marked with the
     color red. Right-click to select the line; then, click **Failure status** to view the
     problem cause.
  3. Select **Edit** to edit the path. Type in a valid path. If changing the path does
     not resolve the problem, select **Remove from repository (with snapshots
     relocation)**.
  4. From the Tools menu, start a rescan of the volume layout.

- There is a corrupted repository. If the repository is corrupted, one of the following error messages might be displayed: FBSS7523E or FBSS7519E. To resolve these errors, you can run **CHKDSK** to repair damaged or corrupted repository files. **CHKDSK** can be run only if snapshots are not running.

  To run **CHKDSK**, complete the following steps:

Procedure

1. Go to **Configuration Tab** > **General Configuration** > **Storage pool** > **Repository Pool**.
2. From the lower left pane, select a disk.
3. Right click a disk; then, click **Run Check Disk**. **CHKDSK** does not run on repository folders.

   Do not run **CHKDSK** from a FastBack Manager system that is installed on a different operating system and NTFS version than the system where the snapshot was taken. For example, a snapshot taken from a Windows Server 2008 system or Windows Vista system cannot be repaired by **CHKDSK** in FastBack Manager on a Windows Server 2003 system.

   Run **CHKDSK** for a snapshot that is taken from a system that is running a supported Windows 2008 or Windows Vista operating system. To initiate this scan, mount the snapshot to a FastBack Client system that is running a supported Windows 2008 or Windows Vista operating system. You can run the **CHKDSK** scan from the FastBack Client system.

4. For all policies that have snapshots stored on the repository, run a checkpoint snapshot. To run a checkpoint snapshot, complete the following steps: Locate**General Configuration** > **Storage pool** > **Repository Pool**in the Configuration tab, right-click the wanted policy, and select **Run Incremental Snapshot**, **Run Checkpoint**, or **Run Full Snapshot**.

   a. From FastBack Manager, go to the **Configuration Tab**.

   b. In the navigation tree, locate the policies.

   c. Right click to select a policy; then, click **Run Check Point**.

Results

By default, when you run **CHKDSK**, it runs in read-only mode. **CHKDSK** is running in read mode to avoid the accidental deletion of snapshot files. If **CHKDSK** fails, you can run **CHKDSK** in write mode. To run **CHKDSK** in write mode, complete the following steps:

1. Identify the drive letter for the failed volume in the repository pool window.
2. Go to the Snapshots Monitor window and verify that no snapshot is currently running. If a snapshot is currently running, either wait for it to complete, or manually terminate it.
3. Verify that no other background process is currently running, for example, cleanup and repository claim.
4. From Windows, click **Start** > **Run**.
5. Enter `cmd`.
6. Enter the following command to stop the FastBack Server:

   `net stop FastBackServer`
7. Enter the following command to run **CHKDSK**:

   `Chkdsk [drive letter] /F`
8. Enter the following command to restart the FastBack Server: `net start FastBackServer`

What to do next

If the previous steps do not resolve the problem, you can try the following options:
- Make sure that all repository locations are accessible from the FastBack Server.
- Check the log for messages that include repair instructions.
- Use the **Claim Repository** option to take ownership of a repository that belongs to another system.

Viewing software versions

Software version information for each component or device is available for display. Use the following methods to access version information:
- FastBack Manager: **Help** > **About**
- FastBack Server: Right-click a server that is at the beginning of the tree pane; then, click **Properties**
- FastBack Client: Right-click a client that is listed under the Storage Pool; then, click **Properties**

Note: A message indicates that the versions of the system elements do not match. For example, the FastBack Manager or the FastBack Client versions are not compatible with the FastBack Server version.

Multi-language support limitations

Tivoli Storage Manager FastBack supports installation of component on non-English version of Windows, in addition to non-ASCII objects (for example, host names, volume names, user names, passwords, and policies).

The updates to Tivoli Storage Manager FastBack for Version 5.5.4 are displayed in English-only. Although the interfaces updated to respond to a defect or problem report, are English-only, the fixes work in all locales.

The reports and any interfaces for FastBack Reporting are displayed in English only. Although the interfaces for FastBack Reporting, and any interfaces updated to respond to a defect or problem report for Version 5.5.4, are English-only, FastBack Reporting and fixes work in all locales.

The following limitations apply to the multi-language support:
- FastBack DR Hub Server supports branches named by using only ASCII characters.
- A repository must be in a folder named by using only ASCII characters.
- Tivoli Storage Manager FastBack products display multi-language characters correctly only if the corresponding font is installed. For example, FastBack Mount can display a policy name in Spanish only if the font used to display characters in the Spanish language are already installed on the system that runs FastBack Mount.
- Computer names have to contain ASCII characters and only one international language. For example, Chinese and English is supported, while Chinese and Hebrew is not supported.
- FastBack Client and FastBack Mount can communicate with an FastBack Server domain name with multi-language characters only if they support the same multi-language encoding.

> **Note:** In case you cannot establish communication, connect by IP instead of computer name.

- The Administrative Command Line supports multi-language input within a UTF-8 encoded script file, and not with command line input. Use the `-s` (script file) option to refer to the script file.
- Tivoli Storage Manager FastBack for Bare Machine Recovery: The FastBack PE share repository browse dialog does not display host names with multi-language characters correctly. In addition, repository share user names and passwords are to be in English.
- Oracle10g script is supported with an English SYSDBA user name.

Chapter 8. Reporting (Windows only)

You can use FastBack Reporting to summarize how repositories, policies, and snapshots consume resources in your network environment. For example, you can prepare an executive summary to identify the successful and failed backups and size of backups, along with a summary of the repository usage.

You can create the following types of reports:

Executive size summary
> This report uses a bar chart to represent the size of backups. A repository summary is also provided.

Executive count summary
> This report uses a bar chart to represent the number of backups per week. The status of the backups, either success or failure, is noted. A table also summarizes the backup size for the most recent day, week, and month.

Detail failures by protected server
> This report provides information about failed snapshots for a specific server.

Repository usage by policy
> This report uses a pie chart and table to represent how much space is consumed by different policies.

Capacity usage by protected server
> This report uses a pie chart and table to represent how much space is consumed by the servers. You can use this report to determine percentage used by this server with respect to total usage.

Initial usage by protected server
> This report uses a bar chart to represent full initial backup of the server.

Storage usage by protected server
> This report uses a table to summarize, for each server, the volumes identified for the server, the volume ID, the capacity volume size, and the backup size.

Volume summary by protected server
> This report uses tables to identify the policies associated with a server and volume, the size of the policy, the number of snapshots stored for the policy, the total snapshot size, the average differential size, and percentage of increase for these snapshot sizes.

Snapshot metrics
> This report uses tables to identify a server, policy, volume, and snapshot. For each snapshot that is taken for the server, policy, and volume combination, there is information about the start time, end time, type, size, percentage change, interval, and status for the snapshot.

Policy summary by protected server
> This report uses tables to present a summary of policies that are run for specific server. You have to select start and end dates, servers, policies, and snapshots to generate the report.

Snapshot size summary by policy
> This report uses a line graph to display the size of snapshots on a specific

day. The snapshot size is measured in GB. You have to select the dates, server, policy, and snapshots to generate the report. In addition, this report provides minimum, maximum, and average size in GB for each server.

Snapshot throughput summary by policy
This report uses a line graph to display the snapshot throughput. The throughput is measured in MB per second, according to a range of dates. You have to select the dates, server, policy, and snapshots to generate the report.

All reports are created in English.

To create and view reports, complete the following steps:

1. Complete the installation process. For installation instructions, see "Installing FastBack Reporting (Windows only)" on page 56.
2. Start the Tivoli Common Reporting Server. For instructions related to starting and configuring the Tivoli Common Reporting Server, see "Starting FastBack Reporting (Windows only)" on page 79.
3. During the installation process, if you change the default installation location, you have to configure the data source. For instructions related to configuring the data source, see "Configuring the data source (Windows only)."
4. Run and view reports. For instructions related to running and viewing reports, see "Running and viewing reports (Windows only)" on page 191.

Configuring the data source (Windows only)

If you use the default installation directory, you do not have to configure the data source.

Before you begin

However, if you change the default installation location (for example, if you change `C:\ProgramFiles\Tivoli\TSM\FastBack\Reporting` to `D:\ProgramFiles\Tivoli\TSM\FastBack`), you must configure the data source. If you change the data source for one report, the change affects all reports. You do not have to configure the data source for each report.

About this task

To configure the data source for a report, complete the following steps:

Procedure

1. From the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Browser**.
2. In the browser window, a message displays a warning about the website security certificate. Continue to the website.
3. Type the user ID and password you set during the Tivoli Common Reporting installation process.
4. Click **Log in**.
5. In the navigation pane, click the **+** icon next to **Reporting** to expand the tree.
6. Click **FastBack Reporting**. In the pane next to the tree, FastBack Reporting information is displayed. The default view is a Navigation tab with `Report Sets` as the root.

7. Click the **+** icon next to **Report Sets** > **Tivoli Products** to expand the tree. Select **FastBack Reporting**.

8. From the table of reports, right-click a report; then, click **Data Sources** from the pop-up menu.

9. Select the **FastBackDataSource** data source and click **Edit**. The FastBackDataSource data source is a database. When the database is identified, the software can query data necessary to generate the report.

10. Change the *JDBC URL column to your database. The JDBC URL looks like the following example: *jdbc:derby:C:\Program Files\Tivoli\TSM\FastBack\reporting\database\FBHDB*

    The database location is relative to your FastBack Reporting installation directory. You must change the following part of the path to match your installation directory: *C:\Program Files\Tivoli\TSM\FastBack\reporting*

11. Click **Save**.

Running and viewing reports (Windows only)

There are two ways to run a report. You can run and view an on-demand report, or you can create a schedule for when the report runs.

About this task

To run an on-demand report, complete the following steps:

Procedure

1. From FastBack Manager, select **Tools** > **Launch Tivoli Common Report**.

2. In the browser window, a message displays a warning about the website security certificate. Continue to the website.

3. Type the user ID and password you set during the Tivoli Common Reporting installation process.

4. Click **Log in**.

5. In the navigation pane, click the **+** icon next to **Reporting** to expand the tree. There is an entry for Common Reporting.

6. Select **Common Reporting**.

7. In the navigation pane, click the **+** icon next to **Report Sets** to expand the tree.

8. In the navigation pane, click the **+** icon next to **Tivoli Products** to expand the tree.

9. In the navigation pane, select **FastBack Reporting**.

10. From the table of reports, right-click a report; then, click **View As** from the pop-up menu. You can select one of the following formats for viewing:
    - HTML
    - PDF
    - Microsoft Excel

      In the Microsoft Excel format, the reports include table data. If there is supposed to be a chart that is provided with the report, on the *Chart* tab, there are data points, but no chart. From the *Chart* tab, go to the menu bar and select **Insert** > **Chart**. The Chart Wizard is displayed. You can use this wizard to create a chart.

      In addition, when you view a report in Microsoft Excel, the default view might seem small and difficult to read. You can use the Microsoft Excel toolbar to change the zoom setting. Changing the zoom setting does not

affect printing. For more information about how to change the zoom setting, use the help that is provided with Microsoft Excel.

- Adobe Postscript

The On-Demand Report Parameters window opens.

11. In the On-Demand Report Parameters window, specify values for all report parameters. Report parameters are predefined by the report design.

12. Click **Run** to run the report. Tivoli Common Reporting begins to gather report data. After the process finishes, the formatted report is displayed in a new browser tab or window.

What to do next

To schedule a report to run later, complete the following steps:

1. From the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Browser**.

2. In the browser window, a message displays a warning about the website security certificate. Continue to the website.

3. Type the user ID and password you set during the Tivoli Common Reporting installation process.

4. Click **Log in**.

5. In the navigation pane, click the **+** icon next to **Reporting** to expand the tree.

6. Click **FastBack Reporting**. In the pane next to the tree, FastBack Reporting information is displayed. The default view is a Navigation tab with Report Sets as the root.

7. Click the **+** icon next to **Report Sets** > **Tivoli Products** to expand the tree. Select **FastBack Reporting**.

8. From the table of reports, right-click a report; then, click **Parameters** from the pop-up menu. The Report Parameters window opens.

9. In the Report Parameters window, specify values for all report parameters. Report parameters are predefined by the report design.

10. Click **Save**.

11. To schedule a report to run, from the table of reports, right-click a report; then, click **Schedules** from the pop-up menu. The Report Schedules window opens.

12. Click **Schedule Snapshots**. The Create Report Schedule window is displayed. There are two tabs in the window: Report Parameters and Schedule.

13. (Optional) Edit report parameters.

14. Click the **Schedule** tab. Complete the fields to schedule the report. For more information about the fields, see the *Tivoli Common Reporting User's Guide*. This document is available online athttp://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.tivoli.tcr.doc/ctcr_intro.html.

15. Click **OK**.

16. In the Report Schedules window, the schedule you created is displayed in a table. Click **OK**.

Problem determination (Windows only)

If there is a problem when you run FastBack Reporting, you need to enable detailed logging in the Tivoli Common Reporting application.

About this task

For more information about this topic, including the path to the log and trace files, see the *Troubleshooting for reports* topic in the *Tivoli Common Reporting User's Guide* , available online at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/ com.ibm.tivoli.tcr.doc/ttcr_logtrace.html.

After you locate the log and trace files, before you contact support, locate a copy of the `HM_HISTORY.CSV` file. The default path to this file is `C:\Program Files\Tivoli\TSM\FastBack\Reporting\bin`. It also helps if you provide support with a screen capture of the window that is displayed when you select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Browser**.

If you receive a fix that applies to FastBack Reporting, to install the fix, complete the following steps:

Procedure

1. Undeploy the history manager. To undeploy the history manager, complete the following steps:
    a. From the Windows Start menu, select **Programs** > **FastBack** > **Reporting** > **Withdraw History Manager**. A DOS command window displays the progress.
    b. During the withdraw history manager process, a window requesting logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password specified during the Tivoli Common Reporting installation process.
    c. Click **OK**.
    d. In the DOS command window, when the deploy history manager process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.
2. Delete the report package. To delete the report package, complete the following steps:
    a. From the Windows Start menu, select **Programs** > **FastBack** > **Reporting** > **Delete Report Package**.
    b. During the delete report package process, a window requesting logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password specified during the Tivoli Common Reporting installation process.
    c. Click **OK**.
    d. In the DOS command window, when the delete report package process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.
3. Launch the executable file to install the FastBack Reporting fix.
4. Stop the Tivoli Common Reporting Server. To stop the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Stop Tivoli Common Reporting Server**.

5. Start the Tivoli Common Reporting Server. To start the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Server**.

6. Update the history manager. To update the history manager, complete the following steps:

   a. From the Windows Start menu, select **Programs** > **FastBack** > **Reporting** > **Update History Manager**. A DOS command window displays the progress.

   b. During the update history manager process, a window requesting logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password specified during the Tivoli Common Reporting installation process.

   c. Click **OK**.

   d. In the DOS command window, when the deploy history manager process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.

7. Import the report package. To import the report package, complete the following steps:

   a. From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **Reporting** > **Import Report Package**. A DOS command window is opened and displays the progress.

   b. During the import report package process, a window requesting logon credentials is displayed. Type the user name and password you use to log on to the Tivoli Common Reporting Server. The user name and password for Tivoli Common Reporting are set during the installation process for Tivoli Common Reporting. The default user name is *tipadmin*. Use the password specified during the Tivoli Common Reporting installation process.

   c. Click **OK**.

   d. In the DOS command window, when the import report package process is complete, press any key to close the window. If an error occurs, a message is displayed in the command window.

8. Stop the Tivoli Common Reporting Server. To stop the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Stop Tivoli Common Reporting Server**.

9. Start the Tivoli Common Reporting Server. To start the Tivoli Common Reporting Server, from the Windows Start menu, select **Programs** > **Tivoli Common Reporting** > **Start Tivoli Common Reporting Server**.

10. Start FastBack Reporting. From FastBack Manager, select **Tools** > **Launch Tivoli Common Report**.

What to do next

After you start FastBack Reporting, you can, if necessary, configure the data source and run reports. For instructions related to configuring the data source, see "Configuring the data source (Windows only)" on page 190. For instructions related to running and viewing reports, see "Running and viewing reports (Windows only)" on page 191.

Chapter 9. FastBack Disaster Recovery (Windows only)

FastBack Disaster Recovery is a remote office data protection system that provides replication and disaster recovery to remote paths.

Each FastBack Server can implement disaster recovery to only one FastBack DR Hub Server.

A replicated repository can be used to back up snapshots to tape and to implement disaster recovery.

FastBack Disaster Recovery can use the following repository sources:

- FastBack - A repository that is divided across several volumes.
- Local - A repository that is in a single folder.
- Network - A repository that is on a network share (for example, \\computer\share\...)

FastBack Disaster Recovery uses the FTP protocol for the disaster recovery destination. FTP is used to create a repository that is on an FTP server. Using the FTP protocol, data can be sent over a regular FTP connection, or FTP over a secure connection, using SSL.

Setting up FTP for the disaster recovery destination (Windows only)

When using FTP for the disaster recovery destination, there are some configuration tasks to complete.

About this task

After you install FastBack DR Hub Server and before using FTP for the disaster recovery destination, complete the following steps. For FastBack DR Hub Server installation instructions, see "Installing FastBack DR Hub Server (Windows only)" on page 50.

Procedure

1. Configure your FTP server. To configure the FTP server, complete the following steps:
   a. Select the *home directory* tab and designate the DR repository directory as a *home* directory for FTP functions.
   b. After designating the DR repository directory you have to change the rights for the home directory from *read only* to *all*.
   c. Configure a local account within the FTP program. This account and password are used by the remote FastBack Servers to communicate with the FastBack DR Hub Server.
2. Open the `FastBackDRHubServer.ini` file for editing. The `FastBackDRHubServer.ini` file is located in the following path: `%ProgramFiles%\Tivoli\TSM\FastBack\drhub`. Make the following changes to the `FastBackDRHubServer.ini` file:
   a. Change the value of the **FTPRootPath1** key to include the full path of the FTP server root directory that was created in step 1

b. (Optional) If needed, add additional directories. For example, *FTPRootPath2* and *FTPRootPath3*.

   c. Change the value for the **ListenPath1** key to contain the full path of the FTP server root directory that was create in step 1 on page 195

   d. (Optional) If needed, add additional directories. For example, *ListenPath2*, *ListenPath3*.

   e. Save and close the `FastBackDRHubServer.ini` file.

3. Restart the Windows service for the FastBack DR Hub Server.

4. In the FTP server root directory that was created in step 1 on page 195, create the following folders:

   - `Logs`
   - `Logevents`

5. For each branch that is required to complete Disaster Recovery to this FastBack DR Hub Server, create a `REP_`*BranchName* folder. The *BranchName* part of the name must match the value stored on the FastBack Manager Disaster Recovery Configuration tab, in the **Branch Name** field. For more information about this field, see "Configuring FastBack Server Disaster Recovery with an FTP server" on page 202.

Configuring Tivoli Storage Manager FastBack Wide Area Network deduplication

Wide Area Network (WAN) deduplication requires configuration tasks to be completed for the Tivoli Storage Manager server, FastBack Server, and FastBack DR Hub Server.

Before you begin

This configuration procedure requires these three tasks to be completed:

1. Configuring the Tivoli Storage Manager Server
2. Configuring the FastBack DR Hub Server
3. Configuring the FastBack Server

Four server systems are referenced in this procedure. The name that is used to identify each of these systems is provided in the following table.

Table 31. Systems used in Configuring Tivoli Storage Manager FastBack Wide Area Network deduplication procedure

Server Type:	Server Name:	Minimum components installed:
FastBack Server	FBserver1	• FastBack Server • FastBack Manager • FastBack DR
FastBack Server	FBserver2	• FastBack Server • FastBack Manager • FastBack DR
FastBack DR Hub Server	FBDRserver	FastBack DR Hub Server
Tivoli Storage Manager server	TSMserver	TSMserver

FastBack Disaster Recovery with Tivoli Storage Manager WAN data deduplication requires the following Tivoli Storage Manager settings:

- The deduplication option for any destination storage pool that is used in FastBack Disaster Recovery WAN Deduplication must be set to `yes`.
- The deduplication option for all nodes that are used in FastBack Disaster Recovery WAN Deduplication must be set to *clientorserver*.
- Make sure the files to be included in data deduplication are not excluded from Tivoli Storage Manager client deduplication processing. See the client exclude.dedup option settings for details. By default, all files are included.

1. Configuring the Tivoli Storage Manager server

Before you begin

Use the following information when you are configuring the Tivoli Storage Manager server `maxsessions`, `mountlimit`, and `maxnummp` options:

- Maximum sessions started during Disaster Recovery replication is sum of the following numbers:

    Maximum number of sessions that are started by each FastBack Server: `num_agent_threads * 3`.

    Maximum number of sessions that are started by the FastBack DR Hub Server: `(4 * num_branches * num_agent_threads) + (6 * num_branches)`.

- Maximum number of sessions for FastBack Mount, instant restore and Tivoli Storage Manager FastBack for Bare Machine Recovery: one session each (or n, where n represents each different node name used). Additional sessions can be used for instant restore operations that are running in parallel.
- Maximum number of sessions that are started by Central Control Station: n (where n equals the number of different nodes).
- The maximum number of mount points that are required is related to the maximum number of sessions. For Disaster Recovery replication, a single session can open one or more volumes. More than one volume is open for a session when the amount of data that is replicated causes a volume to exceed the `MAXCAPACITY` specified for the device class.
- For FastBack Mount, instant restore and Tivoli Storage Manager FastBack for Bare Machine Recovery: The number of mount points that are required for each restore session is dependent on what volumes the required data is on. In a deduplicated storage pool, it is not unusual for the required data to be spread across many volumes.

About this task

These tasks must be completed on Tivoli Storage Manager server version 6.2 (or later).

Procedure

1. On the Tivoli Storage Manager server, define a domain to use for Tivoli Storage Manager FastBack WAN deduplication. FBWAN is used as the domain name:

    `define domain FBWAN`

2. Define a policy set for this domain. FBWANPS is used as the policy set name:

    `define policyset FBWAN FBWANPS`

3. Define a management class for this policy set. FBWANMC is used as the management class name:

```
define mgmtclass FBWAN FBWANPS FBWANMC
```

4. Define a FILE device class. FBWANDC is used as the device class name:

```
define devclass FBWANDC devtype=file mountlimit=256 dir=f:\tsm,g:\tsm
```

This example identifies `f:\tsm` and `g:\tsm` as the directory locations for the device class FBWANDC.

Note: Take the following information into consideration when you configure the `mountlimit` variable:

- The maximum number of mount points that are required is related to the maximum number of sessions. For Disaster Recovery replication, a single session can open one or more volumes. More than one volume is open for a session when the amount of data that is replicated causes a volume to exceed the `MAXCAPACITY` specified for the device class.
- For FastBack Mount, instant restore and Tivoli Storage Manager FastBack for Bare Machine Recovery: The number of mount points that are required for each restore session is dependent on what volumes the required data is on. In a deduplicated storage pool, it is not unusual for the required data to be spread across many volumes.

5. Define a storage pool for the copy group. FBWANSP is used as the storage pool name:

```
define stgpool FBWANSP FBWANDC maxscratch=number duplicate=yes
```

The value for *maxscratch* specifies the maximum number of scratch volumes that the Tivoli Storage Manager server can request for this storage pool. For more information, see the *Tivoli Storage Manager Server Administrator's Reference*. To use either of the Tivoli Storage Manager server side or client-side (WAN) deduplication, `deduplicate=yes` must be specified.

Tip: If you prefer to use deduplication without defining a copy storage pool, issue this command as the Tivoli Storage Manager administrator:

```
setopt deduprequiresbackup no
```

6. Define a copy group for the management class. The default STANDARD copy group is used:

```
define copygroup FBWAN FBWANPS FBWANMC destination=FBWANSP
```

7. Assign management class FBWANMC as the default management class:

```
assign defmgmtclass FBWAN FBWANPS FBWANMC
```

8. Activate the FBWANPS policy set:

```
activate policyset FBWAN FBWANPS
```

9. Register the following Tivoli Storage Manager nodes to the FBWAN domain:

   a. Register the node for each FastBack Server that replicates to the FastBack DR Hub Server (FBserver1, FBserver2). Also, specify the parameters with each command:

   ```
   register node FBserver1 FBserver1pass maxnummp=100 backdel=yes
    deduplication=clientorserver domain=FBWAN
   ```

   ```
   register node FBserver2 FBserver2pass maxnummp=100 backdel=yes
    deduplication=clientorserver domain=FBWAN
   ```

   b. Register the node for the FastBack DR Hub Server (FBDRserver) with these options:

```
register node FBDRserver FBDRserverpass maxnummp=100 backdel=yes
deduplication=clientorserver domain=FBWAN
```

Note: Take the following information into consideration when you configure the `maxnummp` variable:

- The maximum number of mount points that are required is related to the maximum number of sessions. For Disaster Recovery replication, a single session can open one or more volumes. More than one volume is open for a session when the amount of data that is replicated causes a volume to exceed the `MAXCAPACITY` specified for the device class.

- For FastBack Mount, instant restore and Tivoli Storage Manager FastBack for Bare Machine Recovery: The number of mount points that are required for each restore session is dependent on what volumes the required data is on. In a deduplicated storage pool, it is not unusual for the required data to be spread across many volumes.

10. Grant proxy node status to the FastBack DR Hub Server node (FBDRserver). This action allows the FastBack DR Hub Server node (FBDRserver) to operate as a proxy node for the FastBack Server nodes (FBserver1, FBserver2):

    `grant proxynode target=FBserver1 agent=FBDRserver`

    `grant proxynode target=FBserver2 agent=FBDRserver`

11. Set the maximum number of active sessions that are allowed to the Tivoli Storage Manager server:

    `setopt maxsessions 1000`

    Note: Take the following information into consideration when you configure the `maxsessions` variable:

    - Maximum sessions started during Disaster Recovery replication is sum of the following numbers:

        Maximum number of sessions that are started by each FastBack Server: `num_agent_threads * 3`.

        Maximum number of sessions that are started by the FastBack DR Hub Server: `(4 * num_branches * num_agent_threads) + (6 * num_branches)`.

    - Maximum number of sessions for FastBack Mount, instant restore and Tivoli Storage Manager FastBack for Bare Machine Recovery: 1 session each (or n, where n represents each different node name used). Additional sessions can be used for instant restore operations that are running in parallel.

    - Maximum number of sessions that are started by Central Control Station: n (where n equals the number of different nodes).

Results

The Tivoli Storage Manager server is now configured for WAN deduplication.

2. Configuring the FastBack DR Hub Server
Before you begin

FastBack DR Hub Server configuration defines settings that reflect your WAN deduplication environment.

Important:

If the FastBack DR Hub Server is upgraded from Version 6.1.0.x, make sure the IBM Global Security Kit (GSKit) 8 registry key `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK8\CurrentVersion\CryptLibPath` specifies `C:\Program Files\IBM\GSK8\lib` before proceeding.

Do not change the values of the following `DRHubConfigurator.exe` options when you are configuring the FastBack DR Hub Server for WAN deduplication:

```
2 - Set number of Expanding Threads.
3 - Set number of Agent Threads.
4 - Set Xmount Sync Time.
5 - Set Temporary Folder.
```

About this task

Procedure

1. Start the `DRHubConfigurator.exe` utility by clicking **Start**→**All Programs**→**Tivoli Storage Manager** →**FastBack**→**DRHubConfigurator**. Enter the appropriate values for the following `DRHubConfigurator.exe` options:

   a. When the configurator displays `1 - Move Location type to LOCAL`, then the current location setting is `TSM`. `TSM` is the correct value. Therefore, do not change this setting.

   b. `6 - Set TSM server:`
      Specify the host name or IP address of the Tivoli Storage Manager server. (TSMServer)

   c. `7 - Set TSM port:`
      Enter the port number that is used for TCP/IP communication with the Tivoli Storage Manager server. The default value is 1500.

   d. `8 - Set TSM hub node:`
      Enter the node name that is associated with the FastBack DR Hub Server (FBDRserver).

   e. `9 - Set TSM password:`
      Enter the password for the node name that is associated with the FastBack DR Hub Server (FBDRserverpass).

   f. `10 - Add TSM branch node:`

      1) Enter the node name that is associated with the first FastBack Server (FBserver1).

      2) Enter the node name that is associated with the second FastBack Server (FBserver2).

   g. `11 - Remove TSM branch node:`
      Enter the node name that is associated with the FastBack Server to be removed.

   h. `12 - Show current TSM branch nodes:`
      Displays the current FastBack Server nodes in your environment.

   Note the following characteristics in this `FastBackDRHubServer.ini` example:
   - All of the options are preceded by the `[General]` stanza at the beginning of the file.
   - The configuration `TSMDedup=no` is correct.
   - All lines that begin with a semicolon (;) are comments.

```
; FastBackDRHubServer.ini
[General]
LocationType = TSM

Expanding Threads = 5
Agent Threads = 5
Xmount Sync Time = 4

TSMServer=TSMServer
TSMPort=1500
TSMNode=FBDRserver
TSMPasswd=FBDRserverpass
TSMPasswdEncrypted=no
TSMDedup=no
TSMBranchNode1=FBserver1
TSMBranchNode2=FBserver2
```

2. Restart the FastBack DR Hub Server service.
3. Verify that no errors occurred by viewing the contents of the FastBack DR Hub Server log file (FAST_BACK_DR_SERVER_*number*.sf). This log file is in the following path: C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\drhub

```
[Apr 29 13:31:45:000]( c14)->I6.DR        : **************************************
[Apr 29 13:31:45:000]( c14)->I6.DR        : FastBack DR Hub Server started
[Apr 29 13:31:45:000]( c14)->I6.DR        : **************************************
[Apr 29 13:31:45:000]( c14)->I6.DR        : Starting DR Hub server
```

4. Verify that the FastBack DR Hub Server is communicating with the Tivoli Storage Manager server by issuing the query sessions command on the Tivoli Storage Manager server (TSMserver). This command displays active communication sessions to the Tivoli Storage Manager server: This query session output shows that the Tivoli Storage Manager server (TSMserver) is using several sessions to communicate with FBserver1 (FBDRserver).

```
TSM:TSMserver>
query session
```

Sess Number	Comm. Method	Sess State	Wait Time	Bytes Sent	Bytes Recvd	Sess Type	Platform	Client Name
99	Tcp/Ip	IdleW	6.1 M	2.0 K	785	Node	WinNT	FBserver1 (FBDRserver)
100	Tcp/Ip	IdleW	6.1 M	7.3 K	641	Node	WinNT	FBserver1 (FBDRserver)
101	Tcp/Ip	IdleW	6.1 M	1.1 K	1.1 K	Node	WinNT	FBserver1 (FBDRserver)
102	Tcp/Ip	IdleW	6.1 M	1.2 K	493	Node	WinNT	FBserver1 (FBDRserver)
103	Tcp/Ip	IdleW	6.1 M	1.1 K	367	Node	WinNT	FBserver1 (FBDRserver)
104	Tcp/Ip	IdleW	0 S	47.7 K	55.6 K	Node	WinNT	FBserver1 (FBDRserver)
105	Tcp/Ip	IdleW	0 S	237.4 K	47.7 K	Node	WinNT	FBserver1 (FBDRserver)
106	Tcp/Ip	IdleW	0 S	116.5 K	56.6 K	Node	WinNT	FBserver1 (FBDRserver)
107	Tcp/Ip	IdleW	0 S	219.5 K	57.4 K	Node	WinNT	FBserver1 (FBDRserver)

Results

The FastBack DR Hub Server is now configured for WAN deduplication.

3. Configuring the FastBack Server
About this task

This task uses the FastBack Manager GUI.

Procedure

1. Go to **Configuration** > **General Configuration** in the FastBack Manager GUI. Select the **DR Configuration** tab.
2. In the DR target type section, select **TSM**.

3. In the DR parameters section, specify these values:
   - **TSM server address**
     a. **Host name or IP:** Enter the host name or IP address of the Tivoli Storage Manager server (TSMserver).
     b. **Port:** Enter the port number that is used for TCP/IP communication with the Tivoli Storage Manager server. The default value is 1500.
   - **TSM server credentials**
     a. **Node name:** Enter the node name (of the FastBack Server) used to access the Tivoli Storage Manager server (FBserver1). This name is the same one that is used when you configure the FastBack DR Hub Server, specified in the TSMBranchNode1 field.
     b. **Password:** Enter the password that is associated with this node (FBserver1pass).
     c. **As node name:** Leave this field blank.
   - **Branch name**
     Enter the branch name of the FastBack Server (FBserver2).
4. Click **Apply** to save the configuration settings.
5. Click **Test Configuration** to check connectivity to the Tivoli Storage Manager server. Running the configuration test confirms that Disaster Recovery is operational. After the configuration test is complete, a status message is displayed. If configuration is correct, this message displays:

```
DR test configuration completed successfully
```

If an error message displays, complete troubleshooting actions and test the configuration again.

Configuring FastBack Server Disaster Recovery with an FTP server

Disaster Recovery configuration is required for each FastBack Server that sends snapshots to the FastBack DR Hub Server.

About this task

For each FastBack Server that sends snapshots to the FastBack DR Hub Server, complete the following steps:

Procedure

1. From FastBack Manager, go to **Configuration** > **General Configuration**. Select the **DR Configuration** tab.
2. In the DR target section, type the replication destination. The replication destination is the location of the FTP server.
3. In the **Server** field, type either the FTP server name or the FTP IP address.
4. In the Login Credentials section, type the user name and password as they were configured on the FTP server in 1 on page 195.
5. In the **Branch Name** field, type the branch name. The branch name you enter must match the branch name you used for the folder name in the following section: "Setting up FTP for the disaster recovery destination (Windows only)" on page 195. The branch name that you type is not to include the *REP_* prefix.
6. (Optional) To enable Disaster Recovery compression, select **Compression**. This option is to be used if the connection speed is less than 40 Mbps.

7. (Optional), To enable SSL-based Disaster Recovery encryption, select **Encryption**. The FTP server must support encryption and have SSL enabled.

8. Click **Apply** to save the configuration settings.

9. Click **Test Configuration** to check connectivity to the FTP site. By clicking **Test Configuration**, you confirm that the Disaster Recovery is operational. After the configuration test is complete, a status message is displayed.

Completing a Disaster Recovery full shipment

A full shipment minimizes the processing time that is required for an initial Disaster Recovery.

Before you begin

The initial full FastBack Disaster Recovery snapshot typically contains almost all of the data that is stored on the FastBack Servers. As a result, creating this snapshot across a WAN can require a considerable amount of time to complete. This procedure that is referred as a full shipment, describes how to create the initial Disaster Recovery. The creation is done in a manner that avoids the time and network constraints that are associated with transmitting this initial snapshot across a WAN. It is achieved by

* Creating a local branch copy of the Disaster Recovery data.
* Physically transferring the data to the remote Disaster Recovery site.
* Deploying the data in the remote Disaster Recovery site.

About this task

The same FastBack DR Hub Server supports branches that are used in the full shipment and branches that are not used in the full shipment. A FastBack DR Hub Server that already protects existing branches can be used.

Procedure

1. Prepare the data for the local branch:
   Implement Disaster Recovery to a local FTP server on the same LAN. See "Setting up FTP for the disaster recovery destination (Windows only)" on page 195 for instructions. The FTP storage must be transferable as it is eventually sent to the remote Disaster Recovery site.

   a. Prepare a volume with sufficient storage space to contain the repository for the full branch. Format this volume as an NTFS file system. The volume can be on an attached storage device or a system with spanned disks. Spanned disks must be shown as NetShare. For example:
      `F:\<exported_repository on a portable disk array>`

   b. On a local branch, set up an FTP server that shows the Disaster Recovery repository that is on the volume. For example:
      `F:\<exported_repository>`

   c. Configure a local FastBack DR Hub Server to use the same volume path that is used by the FTP server. For example:
      `F:\<exported_repository>`

2. Create a local branch copy of the Disaster Recovery data:

   a. Configure the FastBack Server Disaster Recovery branch settings to communicate with the local FTP server.

b. Create a directory with the branch name and prefix *rep* in your local Disaster Recovery repository. For example:
`F:\<exported_repository>\rep_branch_name`

c. Run Disaster Recovery for all your Disaster Recovery policies.

d. When the Disaster Recovery operations complete, disable FTP Disaster Recovery on your FastBack Server.

3. Transfer the data to the remote Disaster Recovery site:

a. Stop the local FastBack DR Hub Server.

b. Stop the local FTP server.

c. Transfer the volume that is used by the local FastBack DR Hub Server to the remote Disaster Recovery site.

4. Prepare the remote Disaster Recovery site:

a. Record the Tivoli Storage Manager repository and credentials that are associated with the remote FastBack DR Hub Server: For example:
```
"TSM;TCPS:192.168.2.3;TCPP:1500;NODE:hub_node_name;
PASSWORD:1234;FILEPATH:"
```

b. Attach the transferred volume to the FastBack DR Hub Server system. Designate the volume as either an additional drive (that uses an external storage device) or as a shared drive on the system that contains spanned disks.

Important: When you use a network share, do not share the actual rep_branch folder, but share its parent folder. For example:
```
\\some_machine_on_dr_site\exported_repository\rep_branch_name
```

c. Create a node for the branch on the Tivoli Storage Manager server by issuing these commands from the Tivoli Storage Manager server command line:
```
register node node_name password passexp=9999
```
```
update node node_name backdel=yes MAXNUMMP=100 deduplication=clientorserver
```
```
grant proxynode target=node_name agent=hub_node_name
```

Tip: You can create a node name or use the branch name. The hub_node_name is the node that is associated with the FastBack DR Hub Server.

5. Copy the branch data to Tivoli Storage Manager and the remote Disaster Recovery site:

a. Locate the new volume on the FastBack DR Hub Server system. For example:
`F:\dr_repository\rep_branch_name`
or
`\\some_machine_on_dr_site\exported_repository\rep_branch_name`

b. Open a command prompt and navigate to the Tivoli Storage Manager FastBack utilities directory on the FastBack DR Hub Server (`C:\Program Files\Tivoli\TSM\FastBack\utilities`).

c. Copy the branch data into your Tivoli Storage Manager server by using the branch node name and credentials that are defined in Step 4c. For example:
```
.\FBDRCopy.exe -m; "F:\exported_repository\rep_branch_name"
"TSM;TCPS:192.168.2.3;TCPP:1500;NODE:node_name;PASSWORD:1234;FILEPATH:"
```

or
```
.\FBDRCopy.exe -m; "\\some_machine_on_dr_site\dr_repository\rep_branch_name"
"TSM;TCPS:192.168.2.3;TCPP:1500;NODE:node_name;PASSWORD:1234;FILEPATH:"
```

Remember: As shown in these examples, the branch name cannot begin with the `rep_` prefix. Only the source file path begins with the `rep_` prefix.

6. Finalize Disaster Recovery setup on the remote Disaster Recovery site:

   a. Make sure that all shipped branch data is copied into the Tivoli Storage Manager server.

   b. Use the `DRHubConfigurator.exe` utility to update the `TSMNode` parameter (in the `FastBackDRHubServer.ini` file) with the new branch node name.

   c. Restart the FastBack DR Hub Server service.

7. Finalize Disaster Recovery setup on the local branch:

   a. On the FastBack Server for your local branch, modify the Disaster Recovery settings to communicate with the Tivoli Storage Manager server on the remote site. Use the branch node name and credentials that are defined in Step 4c.

   b. Test your settings in the **DR Configuration** window. Click**Apply** and then click **Test Configuration**. A brief delay might occur before test results display.

Results

Your local branch is now protected for Disaster Recovery by the remote FastBack DR Hub Server.

Problem determination for Disaster Recovery (Windows only)

About this task

If there are problems with the Disaster Recovery configuration, complete the following steps to troubleshoot the problems:

Procedure

1. Complete FTP Server configuration. On the FastBack DR Hub Server, an FTP user account must be configured, including a password and a home directory that has full access permissions. The following permissions are required:

   File permissions
   Read, write, delete, and append permissions

   Folder permissions
   Create, delete, list, and add subdirectories permissions

2. Create the three required folders. For more information about the three required folders, see4 on page 196 and 5 on page 196.

3. Complete the configuration required for the `FastBackDRHubServer.ini` file. Configure the FastBack DR Hub Server file to point to the FTP folder root from 1. The default location for the FastBack DR Hub Server file is `C:\Program Files\Tivoli\TSM\FastBack\drhub\FastBackDRHubServer.ini`. For example, make the following changes:

   ```
   ListenPath1 = E:\Path1
   FTPRootPath1 = E:\Path1
   ```

   Uncomment the lines by removing the **;** character.

4. Start the FastBack Disaster Recovery Hub server service. If the previous steps are completed correctly, the following folders are created at the root FTP folder path for the user:

```
E:\path1\receiver_folder
E:\path1\TempMsgFolder
```

In addition, there should be no error messages in the following log files:
`C:\Documents and Settings\All Users\Application Data\Tivoli\FastBack\`
`drhub\FAST_BACK_DR_SERVER_040.sf` (Windows 2003) or `C:\ProgramData\Tivoli\`
`TSM\FastBack\drhub\FAST_BACK_DR_SERVER_040.sf` (Windows 2008 or Windows 7).

The FastBack DR Hub Server is configured.

5. Set up the source FastBack Server to copy snapshot backups, that are in disaster recovery-enabled policies, to the FastBack DR Hub Server. Reference the directions in "Configuring FastBack Server Disaster Recovery with an FTP server" on page 202. Make sure to point to the FastBack DR Hub Server host system and the FTP account set up in 1 on page 205. The name in the **Branch Name** field is critical to ensure that the snapshots are properly identified by the software to the source FastBack Server.

6. Test the FastBack DR Hub Server configuration. Click **Test configuration**. If the configuration is correct, the following actions occur:

   a. Additional folders are, as needed, created in the root FTP path for the user created in 1 on page 205 For example, the following folders are created:
   ```
   E:\Path1\Logs
   E:\Path1\REP_FBServer1
   ```

   The *FBServer1* name is the name specified in the **Branch Name** field.

   b. On the FTP server, several temporary folders and files are created and deleted to test permissions. All files that are created and deleted are part of the test configuration process and is to result in no visible changes to the contents of the folders created in 4 on page 205.

   c. A confirmation message is displayed. The message indicates that the test configuration is successful.

Results

Disaster Recovery configuration is complete and replication operations can begin from the FastBack Server to the FastBack DR Hub Server.

Scheduling replication

Schedule replication for each FastBack Server that sends snapshots to the FastBack DR Hub Server.

About this task

To schedule replication for a FastBack Server, complete the following steps:

Procedure

1. From FastBack Manager, go to **Configuration** > **General Configuration**. Select the **DR Configuration** tab.
2. Click **DR Scheduler** to configure DR scheduling.
3. The default configuration for the DR Scheduler is *Pause*. Configure DR Scheduling and click **Resume**. If you do not click **Resume**, the scheduler does not work.
4. Click **Apply** to complete the configuration.

5. Click **Advanced**.
6. (Optional) The Advanced Job Schedule window provides you with extra scheduling configuration options. Configure the necessary parameters and click **OK**.

Results

Disaster Recovery can require much bandwidth and considerable resources from FastBack Server. FastBack Server activities, including snapshot that is running, can be delayed. Scheduling Disaster Recovery to run during an off-peak time can help reduce the delays.

In addition, do not run replications simultaneously with tape backup or any other activity with extensive FastBack Mount usage, as replication can take longer to complete.

Scheduling bandwidth throttling

You can set the bandwidth throttling to control the rate at which data is transferred from the FastBack Server to the Disaster Recovery (DR) Hub.

About this task

Schedule bandwidth throttling for each FastBack Server to control the rate at which data is transferred from the FastBack Server to the DR Hub.

When bandwidth throttling is not active, data that is transferred over WAN uses the maximum network bandwidth. When bandwidth throttling is active, data is transferred with a limited bandwidth rate so that the network bandwidth is not fully used.

You can set the throttling parameters to achieve these tasks:
- Enable or disable throttling.
- Add throttling events over the assigned time intervals.
- Modify throttling events.
- Remove a throttling event.
- Display DR throttling information.

Enabling bandwidth throttling

If data transfers from the FastBack Server to the DR Hub use the full network bandwidth, enable bandwidth throttling to set limitations on the bandwidth usage.

About this task

To enable bandwidth throttling, complete the following steps:

Procedure

1. Click **Configuration** > **General Configuration** > **DR Configuration** tab.
2. In the **DR target type** section, select **TSM**.
3. Select the **Enable Throttling** check box.
4. In the **Bandwidth Unit** section, use the drop-down menu to select the bandwidth data rate unit. Select one of the following options. The default is kilobytes per second (KBps).

- kbps (kilobits per second.)
- Mbps (megabits per second)
- Gbps (gigabits per second)
- KBps (kilobytes per second)
- MBps (megabytes per second)
- GBps (gigabytes per second)

5. Click **Apply** to enable bandwidth throttling and display the **DR Throttling** tab.

Viewing DR throttling tab

The **DR throttling** tab provides a calendar where throttling events are created, modified, and deleted.

About this task

To view the throttling event calendar, click the **DR Throttling** tab.

- The tab contains a calendar grid. The entire tab is viewable by using scroll bars. The columns and rows are fixed in size.
- The calendar grid displays 7 columns for each day and 24 rows for each hour.
- The throttling event:
  - Is represented by a shaded-color text pane that covers a time interval. The default time interval is one hour and is set for each day.
  - Can cover a minimum time interval of 0.5 hour and up to a maximum interval of a 24-hour day.
  - Uses the same bandwidth unit for all events that is set in the **DR Configuration** tab. For example, if you selected MBps in the **DR Configuration** tab, all the events that are displayed in the **DR Throttling** tab are MBps rates.

    Tip: When you hover the mouse pointer over an event, you can view a tooltip with event information.
- Throttling is not active where events do not exist. Data is transferred at the maximum bandwidth rate.

Adding a throttling event

On the **DR Throttling** tab, add an event to set the time interval and data rate that is used for transferring data. This action controls data transfers to minimize usage of the network load.

About this task

To add a throttling event, click the **DR Throttling** tab, and complete the following steps:

Procedure

1. Select a grid cell on the day (column) and hour (row) where you want to add a throttling event. Right-click the cell and select **Add Event**.
2. From the window, select the **Start** and **End** time interval. You can set each time field so that it can be incremented in 30-minute or 1-hour intervals.
   - The default value of the hour interval depends on the grid cell location that you clicked.

- The time format uses the default locale format (for example, 24 hour or AM/PM)
3. In the **Rate** field, enter an integer number. Alternatively, use the scroll bar for the input field to increase or decrease the value by single units.
4. Click **Apply** to add the throttling event.

Modifying a throttling event

After you create an event, you can modify an event to set different throttling values.

About this task

To modify a throttling event, click the **DR Throttling** tab and complete the following steps:

Procedure

1. Select a throttling event and right-click the event. Click **Modify Event**. A window displays the (previously selected) values for the **Starts**, **Ends**, and **Throttling rate** fields.
2. Make the necessary changes in the fields.
    a. You can set each time field so that it can be incremented in 30-minute or 1-hour intervals. The time format uses the default locale format (for example, 24 hour, or AM and PM)
    b. If the **Throttling rate** field displays a zero value, the rate is too small to be displayed for the current unit setting (gbps, GBps). A tooltip displays the actual value when you move the mouse pointer on the zero.
3. Click **Apply** to submit the changes.

Removing a throttling event

When throttling events are no longer necessary and need to be removed, follow this task to remove the event.

About this task

To remove a throttling event, click the **DR Throttling** tab and complete the following steps:

Procedure

1. Select a throttling event and right-click the event. Select **Remove Event**. A window displays event information.
2. Click **OK** to confirm to delete the event.

Disabling bandwidth throttling

If your network requirements improve or change in a way where throttling is not needed, you can disable bandwidth throttling.

About this task

To disable bandwidth throttling, complete the following steps:

Procedure

1. Click **Configuration** > **General Configuration** and click the **DR Configuration** tab.
2. Clear the **Enable Throttling** check box.
3. Click **Apply**. Throttling activity is disabled. The maximum network bandwidth rate is used.

   Note: Throttling events that exist, before throttling is disabled, are not discarded. To view the events, select the **Enable Throttling** check box and click **Apply**.

Displaying throttling information

If throttling is active, you can view general throttling information through the Disaster Recovery icon.

About this task

Hover the mouse pointer over the disaster recovery icon to display disaster recovery information. Throttling information like the current transfer rate and the throttling limit is included.

Using Disaster Recovery

After configuring Disaster Recovery, from FastBack Manager, go to **Configuration** > **General Configuration**. Select the **DR Configuration** tab, you can use Disaster Recovery. The following tasks can be initiated from the DR Configuration tab:

Run Now
> Click **Run Now** to run an immediate, not scheduled, Disaster Recovery backup.

Test Configuration
> Click **Test Configuration** to check connectivity to the FTP site. This action also confirms that the FastBack DR Hub Server is operational. A status message is displayed after the configuration test is complete.

Abort DR
> Click **Abort DR** to stop any currently running Disaster Recovery. For the Disaster Recovery tasks that are running, the Disaster Recovery is aborted after the task is complete, but before the entire Disaster Recovery is finished.

Locking snapshots during Disaster Recovery

Files that are updated during the Disaster Recovery process are categorized as new files, changed files, or deleted files.

When new files are replicated, the new files are immediately copied into the final destination repository. When changed files are replication, the changed filed are initially copied to a temporary folder. When replication to the temporary folder is complete, the changed files are copied to the final destination repository. After the replication process is complete, files that need to be removed from the replicated repository are deleted.

During the replication process for new files, changed files, and deleted files, FastBack Disaster Recovery locks snapshots. As a result, FastBack Mount cannot mount the relevant replicated snapshots.

When FastBack Mount mounts a snapshot, it locks the entire policy, preventing FastBack Disaster Recovery from changing files. When the snapshot is dismounted, the lock is removed. If FastBack Mount is idle for a certain amount of time, FastBack Disaster Recovery can remove the lock. FastBack Disaster Recovery tries to remove locks until all the files are copied.

Central Control Station (Windows only)

The Central Control Station provides you with a graphical user interface to browse the remote repository. This repository serves as the central storage area for the FastBack Disaster Recovery system.

The Central Control Station can be installed at a central backup office or Data Center. You can use the Central Control Station to view the branches that implemented Disaster Recovery and view the status for each branch. In addition, you can start FastBack Manager from the Central Control Station.

Starting Central Control Station (Windows only)
About this task

To startCentral Control Station, click **Start** > **Programs** > **Tivoli Storage Manager** > **FastBack** > **Central Control Station**.

Using Central Control Station (Windows only)

After you start the Central Control Station, connect to a share before any data is displayed. A share is a path location where files are stored for the FastBack DR Hub Server.

To connect to a share, click **File** > **Connect**. The Connect dialog is displayed.

Type or browse for the path to the shared snapshots and shared events. The path to the shared snapshots is the path you used when you created the `Logs` folder during the setup of FTP for the disaster recovery destination. Likewise, the path to the shared events is the path you used when you created the `Logevents` folder. These folders are sub folders under the replication destination folder. For more information, see "Setting up FTP for the disaster recovery destination (Windows only)" on page 195.

If you can access the share in Windows Explorer, with the current operating system user privileges, you do not have to type a user name, password, or domain. If the share is not accessible, type information in these fields to ensure that the Central Control Station can connect to the share.

After you connect to a share, the main window displays a branch tree, and, according to the selection in the branch tree, corresponding snapshot logs and snapshots. At the bottom of the branch tree, there are four buttons that you can select to filter data that is displayed in the Snapshot Log and Snapshot tables. The following list provides details about the buttons:

Day Displays snapshot information for the current day. Unless, in the branch tree, *All branches* is selected, **Day** is the default filter.

Week   Displays snapshot information for the current week.

Month
>Displays snapshot information for the current month.

All   Displays the information from all branches. **All** is disabled if *All branches* is selected in the branch tree. If, in the branch tree, *All branches* is selected, **Month** is the default filter.

The time that is displayed in the Snapshot Log and Snapshot tables is the local time on the branch.

Viewing snapshot information

By default, most of the information about snapshots is displayed near the top of the window in the Snapshot table. You can right-click a row in the table; then, click **Snapshot Log**. A detailed log for the snapshot is displayed.

The snapshot log includes a list of events that are related to the snapshot. This list is helpful for snapshots that did not complete or that failed. The log that is displayed to the customer might not include information about why the snapshot did not complete or failed. In this list, the details about why the snapshot did not complete or failed are to be available.

In the Snapshot Log table, you can sort data by alphabet characters in ascending or descending order, according to a specific column. To sort, click a column header.

Under the Snapshot Log table, there is a Snapshots table. This Snapshots table provides more detail about the snapshots that completed. Status, start time, policy name, volume, and type are some of the details that are provided about the snapshots.

Icons in the Snapshots table might be grayed out. This icon color is used if the **Enable DR** field is set to *no* for the policy.

Refreshing data

You can refresh data that is displayed in the Central Control Station at any time by clicking **View** > **Refresh**. The information automatically updates according to a time parameter that is set for the application.

When data is refreshed, the cursor changes appearance to indicate that data is being updated. When the refresh is complete, the cursor returns to normal appearance.

Starting FastBack Manager from Central Control Station

To start FastBack Manager from Central Control Station, go to the branch tree, in the Central Control Station. Right-click an active branch; then, select **Manage**. When you select **Manage**, a new instance of FastBack Manager is started. You can run more than one instance of FastBack Manager.

Saving settings

When you close the Central Control Station, the sorting settings for tables are stored by the application. In addition, connection information, except for passwords, is saved.

Chapter 10. Administrative Command Line

The Administrative Command Line is a way to access most Tivoli Storage Manager FastBack functions from a command line interface.

The Administrative Command Line can be viewed as a command prompt API (application interface) to FastBack Server and FastBack Mount. Changes completed with the Administrative Command Line to the FastBack Server and FastBack Mount take effect immediately.

You can use the Administrative Command Line to manage only one FastBack Server or one system that is running FastBack Mount.

Restriction: The maximum number of characters allowed for an Administrative Command Line user name, password, or domain name is 31 characters.

Starting the Administrative Command Line

Before you begin

Before you can start and use the Administrative Command Line from a supported Linux operating system, complete the software prerequisites detailed in "Software requirements and prerequisites" on page 33.

About this task

To start the Administrative Command Line, complete the following steps:

Procedure

1. From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **FastBack** > **Administrative Command Line**.
2. In the command prompt window, enter one of the following commands:
   - To run the command line:

     ```
     FastBackShell.exe -c command type tag parameter
     ```
   - (Windows only) To display the help for the command line:

     ```
     FastBackShell.exe -h
     ```
   - (Linux only) To display the help for the command line:

     ```
     FastBackShell.exe -h dump
     ```

     For example, this command displays detailed help on the job command line:

     ```
     FastBackShell.exe -h job dump
     ```
   - To run the command line with a script file to run multiple commands:

     ```
     FastBackShell.exe -s "script_file_name"
     ```

Authentication

After the installation process is complete, change the password for the administrator user name.

The authentications privileges are allocated to the user name and password that you use when you log on. The authentication privileges determine the restore options that you can use. You can override the current security setup by using appropriate switches in Administrative Command Line:

```
FastBackShell.exe -c -u UserName -p Password -d domain job add -jname <xxxxxx>
FastBackShell.exe -s -u UserName -p Password -d domain
```

When you use the -u, -p, and -d switches, the current account is displayed and identified as other login accounts. You can use these switches when there are insufficient permissions to restore a snapshot.

You can also use the built-in administrator credentials:

```
FastBackShell.exe -c -u admin -p admin123 -d xpress-restore
```

Command overview, including reading syntax diagrams

When you use the following commands, all parameters are not required. See the following sections for details about which parameters are required.

For the parameters that are not required and not entered, default values are used. Parameters with spaces must be enclosed in quotation marks. For example, if you want to use the *Accounting, Daily* parameter, type "Accounting, Daily".

To read a syntax diagram for entering a command, follow the path of the line. Read the syntax diagram from left to right, and from top to bottom, and use the following guidelines:

- The >>- character sequence indicates the beginning of a syntax diagram.
- The --> character sequence at the end of a line indicates that the syntax diagram continues on the next line.
- The >-- character sequence at the beginning of a line indicates that a syntax diagram continues from the previous line.
- The -->< character sequence indicates the end of a syntax diagram.

Symbols

Enter these symbols exactly as they are displayed in the syntax diagram:

*	Asterisk
{}	Braces
:	Colon
,	Comma
=	Equal sign
-	Hyphen
()	Parentheses
.	Period
	Space
"	Quotation mark
'	Single quotation mark

Variables

Italicized lowercase items such as *<variable_name>* indicate variables. In this example, you can specify a *<variable_name>* when you enter the **cmd_name** command.

```
►►──-cmd_name──<variable_name>─────────────────────────────────────────►◄
```

Required choices

When two or more items are in a stack and one of them is on the line, you must specify one item. In the following example, you must choose either *A*, *B*, or *C*:

```
►►──-cmd_name──┬─A─┬──────────────────────────────────────────────────►◄
               ├─B─┤
               └─C─┘
```

Optional choices

When an item is below the line, that item is optional. In the following example, you can select either *A* or nothing at all:

```
►►──-cmd_name────────────────────────────────────────────────────────►◄
              └─A─┘
```

When two or more items are in a stack below the line, all items are optional. In the following example, you can choose either *A*, *B*,*C*, or nothing.

```
►►──-cmd_name────────────────────────────────────────────────────────►◄
              ├─A─┤
              ├─B─┤
              └─C─┘
```

alerts

Use the **alerts** command to create, send, and view alerts.

There are three tags that you can use for the **alerts** command: **send**, **create_file**, and **view**. The following list provides detail for these tags:

send Use this tag to send alerts. The following code sample is an example of how to use the tag with the **alerts** command:

```
FastBackShell.exe -c alerts send
```

create_file

Use this tag to create alerts file. The following code sample is an example of how to use the tag with the **alerts** command:

```
FastBackShell.exe -c alerts create_file
```

view Use this tag to view the content of Heart Beat alert emails.

app

Use the **app** command for global parameters configuration.

The following code sample provides detail for the **app** command:

```
FastBackShell -c app view
FastBackShell -c app set (-quiesc [y|n] | -purge [y|n] | -vss [y|n])
```

You cannot specify *y* for both **-quiesc** and **-vss**. You can enable either IBM application quiescing or the VSS service. The VSS service is a type of application quiescing.

client

You can use the **client** command to view information like name, version, and connection status of all FastBack Clients.

Use the following command for the **client** command:

```
client view
```

client_group

Use the **client_group** command to administer client groups.

Use the following format for the **client_group** command:

```
client_group command_type -command_tag
 command_tag_parameter
```

Note: Clients can only be added to client groups using their host name, and not the IP address.

The following list summarizes the types that you can specify for the **client_group** command. Tags and parameters for each type are listed.

add   Use the **add** command type to add a client group. The valid command tags are **-cname** and **-agent**. The **-cname** command tag indicates the client group name. The **-agent** command tag indicates the server mount point. The following examples indicate the format to use:

```
client_group add -cname command_tag_parameter -agent
 command_tag_parameter [-agent
 command_tag_parameter]*n
```

```
client_group add -cname "C and D" -agent winxp-1@C:\ -agent winxp-1@D:\
```

del   Use the **del** command type to delete a client group. The valid command tags are **-cname** and **-all**. The **-cname** command tag indicates the client group name. The **-all** command tag indicates the command runs on all client groups. For the **-all** command tag, specify *y* for yes or *n* for no as the command tag parameter. The following example indicates the format to use:

```
client_group del -cname command_tag_parameter [-all
 command_tag_parameter]
```

edit   Use the **edit** command type to edit a client group. The valid command tags are **-cname** and **-rename** and **-agent**. The **-cname** command tag indicates the client group name. The **-rename** command tag indicates a new client group name should be used. The **-agent** command tag indicates the server mount point. The following examples indicate the format to use:

```
client_group edit -cname command_tag_parameter [-rename
 command_tag_parameter] [-agent
 command_tag_parameter]*n
```

```
client_group edit -cname "C and D" -rename "C on winxp-1" -agent winxp-1@C:\
```

info   Use the **info** command type to access client group status. The valid
command tags are **-cname** and **-request**. The **-cname** command tag
indicates the client group name. The **-request** command tag checks to see
if a specified job exists. The following examples indicate the format to use:

```
client_group info -cname command_tag_parameter -request
 command_tag_parameter
```

```
client_group info -cname "C and D" -request exist
```

view   Use the **view** command type to view a client group. For example:

```
client_group view
```

dr

Use the **dr** command for disaster recovery tasks.

The following format is to be used for the **dr** command:

```
dr -command_Tag
```

The following list summarizes the tags that you can specify for the **dr** command.
Parameters for each tag are listed.

run_now
Disaster recovery starts immediately.

abort   Disaster recovery is terminated immediately.

pause   Pauses disaster recovery. Disaster recovery does not run on a schedule.

resume   Resumes disaster recovery. Disaster recovery runs as scheduled.

test_configuration
Checks the disaster recovery configuration.

is_running
Checks to determine whether the disaster recovery is running.

irestore (Windows only)

Use the **irestore** command to send an instant restore command to FastBack
Mount.

Use the following format for the **irestore** command:

```
irestore -Command_Tag Command_Tag_Parameter
irestore  -target command_tag_parameter  -server command_tag_parameter
 -policy command_tag_parameter -volume command_tag_parameter -date
 command_tag_parameter [-when command_tag_parameter] -rep command_tag_parameter
 [-login command_tag_parameter] [-pass command_tag_parameter]
 [-domain command_tag_parameter] [-force]
```

The following list summarizes the tags that you can specify for the **irestore**
command. Parameters for each tag are listed.

target   Use this tag as the target for instant restore. A drive letter local to FastBack
Mount. Only the first character is used. Only basic volumes are supported.

rep   The FastBack Server repository (local or network share). For local, use
hostname@domain. You can also use the full path for the repository on the
folder. For example: share: '*share*: *hostname**share*'

The **-rep** tag can direct to a Tivoli Storage Manager server . For example:
-rep 'tsm: ip=<*IP address*> port=<*port*> node=<*node*> as node=<*as node*>
pass=<*password*> branch=<*branch*>'

server The server that was the snapshot source or *SAN_layout*.

policy The policy for the snapshot.

volume The volume or reparse point that was the source of the snapshot.

date The date is formatted as *yyyy-Mmm-dd hh:mm:ss* or *last snapshot*. For *yyyy*, the range must be from *1971* to *2030*.

when There are three options: *after*, *before*, or *exact*. The default is *exact*.

login The user name used to access the restored snapshot and target volume.

pass The password used with the **login** command.

domain The domain used with the **login** and **pass** commands. The default is *xpress-restore*.

force Use this command to unmount the target volume when there are open files or running applications.

Sample

See the following sample for an example of how the user can do an instant restore to volume *I:*. The snapshot of the volume *I* is to be completed on a specific server, according to a specific policy, volume, and time. Open files and running applications on the volume, called the target disk, *I* are ignored. The FastBack Server must also be stopped and restarted.

```
-c irestore -target I:\ -server winxp-leon -policy "I_ on winxp-leon at 81
 606 16_49" -volume I:\ -date  "2006-Sep-12 19:29:01" -rep e:\repository
 -login admin -pass admin123 -domain xpress-restore -force
```

job

Use the **job** command to add, edit, delete, and view jobs. You can also access information about job status.

Use the following format for the **job** command:
job *command_type -command_tag command_tag_parameter*

The following list summarizes the types that you can specify for the **job** command. Tags and parameters for each type are listed.

add Use the **add** command type to add a job. The following list provides the valid command tags:

- (Windows only) **-cdp** - Use this tag to set continuous data protection. The choices are *y* for yes and *n* for no.
- **-contentaware** - Use this tag to set the content aware option. The choices are *y* for yes and *n* for no.
- **-exclude** - Indicates a time period to exclude. The format is *from HH:MM to HH:MM*. An example of the **-exclude** tag and parameter follows: -exclude from 21:00 to 07:00
- **-interval** - Indicates the interval for the job, for example, run every hour. The format is *HH:MM*. The default is *0:30*.

You cannot specify the hours that you want the job to run. You must define the interval time. For example, if you want to run the job once every two hours, use the following tag and parameter with the **add** command type: `-interval 2:00`

- **-jname** - Indicates the job name.
- **-occur** - Indicates when the job ends. There are three parameters that you can specify for this tag: *end_by MM-DD-YYYY*, *end_after _NUMBER_*, and *no_end*. Use *end_by MM-DD-YYYY* to specify a specific end date. Use *end_after _NUMBER_* to end after a specified number of times. Use *no_end* for a continuous run. The default is *no_end*.
- **-purge** - Use this tag to specify that the Microsoft Exchange logs should be purged. The choices are *y* for yes and *n* for no.
- **-quiesc** - Use this tag to set the quiescing option. The choices are *y* for yes and *n* for no. Select the *y* option when using a 32-bit machine. For 64-bit machines, select the *n* option. When using a 64-bit machine, set the **-vss** tag to *y*.
- **-schedule** - Indicates when the job is scheduled to run. The format is `Weekly Every _WeeksNumber_ on _DaysBitMap_`.

  You need to specify the *_WeeksNumber_* parameter. Use the default, *1*, to ensure the schedule runs every week.

  For the *_DaysBitMap_* parameter, the software uses a 7–digit binary bitmap representation to specify the days for the schedule. Every number between 1 and 127 represents a set of days, for example:
    - *1* represents *Sunday* (*0000001*)
    - *3* represents *Monday and Sunday* (*0000011*)
    - *32* represents *Friday* (*0100000*)
    - *42* represents *Monday, Wednesday, and Friday* (*0101010*)
    - *62* represents *Monday, Tuesday, Wednesday, Thursday, and Friday* (*0111110*)
    - *127* represents *all days of the week* (*1111111*)

  The default schedule parameter is *Weekly Every 1 on 1*.
- **-start** - Indicates the start time for the job schedule. The default is the current time. The time format is *MM-DD-YYYY HH:MM*. An example of the **-start** tag and parameter follows: `-start "01–19–2008 07:30"`
- **-type** - Indicates the type of job. There are three choices: *inc*, *full*, and *diff*. Use *inc* for an incremental snapshot. Use *full* for a full snapshot. Use *diff* for a differential snapshot, also known as an incremental delta block snapshot. The default type parameter is *inc*, for an incremental snapshot.
- **-vss** - Use this tag to set the VSS service. The choices are *y* for yes and *n* for no. Select the *y* option when using a 64-bit machine. For 32-bit machines, select the *n* option. When using a 32-bit machine, set the **-quiesc** tag to *y*.

The following code sample is an example of how to specify the **add** command type and some of the available tags and parameters for the **job** command:

```
FastBackShell.exe -c -u admin -p admin123 -d xpress-restore job
 add -jname NightTest -interval "00:01" -schedule "Weekly Every 1 on 127"
 -purge n -vss n -contentaware y
```

del   Use the **del** command type to delete a job. The valid command tags are **-jname** and **-all**. The **-jname** command tag indicates the job name. The **-all** command tag indicates the command runs on all jobs. For the **-all**

command tag, specify *y* for yes or *n* for no as the command tag parameter. The following example indicates the format to use:

```
job del -jname command_tag_parameter [-all command_tag_parameter]
```

edit   Use the **edit** command type to edit a job. The following list provides the valid command tags:

- (Windows only) **-cdp** - Use this tag to set continuous data protection. The choices are *y* for yes and *n* for no.

- **-contentaware** - Use this tag to set the content aware option. The choices are *y* for yes and *n* for no.

- **-exclude** - Indicates a time period to exclude. The format is *from HH:MM to HH:MM*. An example of the **-exclude** tag and parameter follows: `-exclude from 21:00 to 07:00`

- **-interval** - Indicates the interval for the job, for example, run every hour. The format is *HH:MM*. The default is *0:30*.

  You cannot specify the hours that you want the job to run. You must define the interval time. For example, if you want to run the job once every two hours, use the following tag and parameter with the **add** command type: `[-interval 2:00]`

- **-jname** - Indicates the job name.

- **-occur** - Indicates when the job ends. There are three parameters that you can specify for this tag: *end_by MM-DD-YYYY*, *end_after _NUMBER_*, and *no_end*. Use *end_by MM-DD-YYYY* to specify a specific end date. Use *end_after _NUMBER_* to end after a specified number of times. Use *no_end* for a continuous run. The default is *no_end*.

- **-purge** - Use this tag to specify that the exchange logs should be purged. The choices are *y* for yes and *n* for no.

- **-quiesc** - Use this tag to set the quiescing option. The choices are *y* for yes and *n* for no. Select the *y* option when using a 32-bit machine. For 64-bit machines, select the *n* option. When using a 64-bit machine, set the **-vss** tag to *y*.

- **-rename** - Indicates the new backup job name. The following sample uses the **-rename** command:

  ```
  FastBackShell.exe -c -u admin -p admin123 -d xpress-restore
   job edit -jname "Old Name" -rename "New Name"
  ```

  The **-jname** argument specifies the job that you are referring to.

- **-schedule** - Indicates when the job is scheduled to run. The format is `Weekly Every _WeeksNumber_ on _DaysBitMap_`.

  You need to specify the *_WeeksNumber_* parameter. Use the default, *1*, to ensure the schedule runs every week.

  For the *_DaysBitMap_* parameter, the software uses a 7–digit binary bitmap representation to specify the days for the schedule. Every number between 1 and 127 represents a set of days, for example:

  - *1* represents *Sunday* (*0000001*)
  - *3* represents *Monday and Sunday* (*0000011*)
  - *32* represents *Friday* (*0100000*)
  - *42* represents *Monday, Wednesday, and Friday* (*0101010*)
  - *62* represents *Monday, Tuesday, Wednesday, Thursday, and Friday* (*0111110*)
  - *127* represents *all days of the week* (*1111111*)

The default schedule parameter is *Weekly Every 1 on 1*.

- **-start** - Indicates the start time for the job schedule. The default is the current time. The time format is *MM-DD-YYYY HH:MM*. An example of the **-start** tag and parameter follows: `-start "01–19–2008 07:30"`
- **-type** - Indicates the type of job. There are three choices: *inc*, *full*, and *diff*. Use *inc* for an incremental snapshot. Use *full* for a full snapshot. Use *diff* for a differential snapshot, also known as an incremental delta block snapshot. The default type parameter is *inc*, for an incremental snapshot.
- **-vss** - Use this tag to set the VSS service. The choices are *y* for yes and *n* for no. Select the *y* option when using a 64-bit machine. For 32-bit machines, select the *n* option. When using a 32-bit machine, set the **-quiesc** tag to *y*.

The following code sample is an example of how to specify the **edit** command type and some of the available tags and parameters for the **job** command:

```
job edit -jname "My Job" -rename "My Old Job"
```

info   Use the **info** command type to access job status. The valid command tags are **-jname** and **-request**. The **-jname** command tag indicates the job name. The **-request** command tag checks to see if a specified job exists. The following examples indicate the format to use:

```
job info -jname command_tag_parameter -request command_tag_parameter
```

```
client_group info -jname "C and D" -request exist
```

view   Use the **view** command type to view a job. For example:

```
job view
```

log

Use the **log** command for log file options.

The following format is to be used for the **log** command:

```
log view -type event -file file_name
```

For example, if you want the event log information to be in the `events.txt` file, enter the following command:

```
log view -type event -file events.txt.
```

mount

Use the **mount** command to complete various FastBack Mount tasks. When you run the **mount** command, use either a Windows logon ID with Administrator authority, or log on to the Linux system as the root user.

The Administrative Command Line, sometimes called the FastBack Shell, can be used to mount (**mount add**) and unmount (**mount del**) volumes, and to view a list of mounted volumes (**mount view**). Because the **mount add** command takes so many command tags, a **mount dump** command is also available. This **mount dump** command generates FastBack Shell commands for scripting purposes.

To use the **mount** command, FastBack Mount must be running. The `FastBackShell.ini` file must contain the name or IP address of the system where FastBack Mount is installed. This information is specified in the *HOSTNAMES* section. The `FastBackShell.ini` file is stored in the installation folder for the Administrative Command Line. The default location is `C:\Program Files\Tivoli\TSM\FastBack\shell`.

Snapshots are mounted or unmounted on the system where FastBack Mount is running. The repository can be shared over the network or attached to a FastBack Server.

The **mount** command is supported in command and script file modes. The following command types are available. The appropriate tags and parameters are listed alongside each command type.

add   Use this command type to mount a snapshot to the system where FastBack Mount is running. The following list identifies the tags and parameters for the **add** type:

- **-target** - This tag is required.

  Use this tag to specify the following targets:
  - (Windows only) Virtual volume
  - (Windows only) Reparse point
  - (Linux only) iSCSI target

  The following examples use the **-target** tag:
  - (Windows only) In the following example *V:* is the virtual volume mount target:

    ```
    -target "V:"
    ```
  -

  - (Windows only) In the following example a reparse point volume mount target is specified:

    ```
    -target "C:\SNOWBIRD@FASTBACK\SnowbirtK\Snowbird\K\\"
    ```
  - (Linux only) In the following example an iSCSI target is specified:

    ```
    -target "ISCSI: target=<target_name> initiator=<initiator_name>"
    ```

- **-rep** - This tag is required.

  Use to specify the local or network share repository. For local repositories, you can specify "*hostname@domain*" or the full path for repository on folder.

  If the repository is on a network share, include the user name, password, and domain for a user, who has access to the network share, in the following format:

  ```
  "<path to network share> user=<username> pass=<password>
    domain=<domain>"
  ```

  <path to network share> can take the form of "*share:\\<hostname>\ <repository name>*" or "*\\<hostname>\<repository name>*". The default name for a repository volume is "*FB_REP_<drive letter>*". The following example uses a network shared repository:

  ```
  -rep "share:\\ftp2-2k3\Share_of_Rep user=administrator pass=12345
    domain=ABC"
  ```

  The **-rep** tag can direct to a Tivoli Storage Manager server. For example:
  ```
  -rep 'tsm: ip=<IP address> port=<port> node=<node> as node=<as
  node> pass=<password> branch=<branch>'
  ```

- **-policy** - This tag is required. Use to specify the policy that includes a snapshot that is used in the backup.

- **-server** - This tag is required. Use to specify server name that is the source for the snapshot. The following example uses this tag with a server name:

  ```
  -server "snowbird"
  ```

You can alternatively use the following parameter: **SAN_layout**.

- **-volume** - This tag is required. Use to specify the volume that is the source of the snapshot. The following example uses *D:* as the source volume:

  ```
  -volume "D:\\"
  ```

- **-date** - This tag is required. Use to specify the date of the snapshot that you want to mount.

  The **-rep**, **-policy**, **-server**, and **-volume** tags specify exactly what volume is to be mounted, but not which snapshot on the volume. Specify the date in the following format: *yyyy-Mmm-dd hh:mm:ss*. Alternatively, specify "*last snapshot*" to mount the most recent snapshot on the volume. The following example uses the *yyyy-Mmm-dd hh:mm:ss* format to specify the date:

  ```
  -date "2008-Sep-20 15:47:35" -when after
  ```

- **-when** - Use to specify when the snapshot is mounted. The three parameter options are *after*, *before*, or *exact*. The default value is *exact*.

- **-login** - Use to specify the user name that is used when mounting. If this tag is not specified, the user that is currently logged on to FastBack Mount is used. Use this tag only with the **-domain** and **-pass** tags.

- **-domain** - Use to specify the domain when mounting. If no domain is specified, by default, the *xpress-restore* domain is used. Use this tag only with the **-login** and **-pass** tags.

- **-pass** - Use to specify the password when mounting. Use this tag only with the **-login** and **-domain** tags.

- **-ro|-fw** - Use to specify whether the mounted volume is read-only (**-ro**) or fake-write (**-fw**).

The following examples indicate how to specify the **add** type, and the corresponding tags and parameters:

- The following example shows how to mount a snapshot from a repository on a network share:

  ```
  mount add -target X: -rep "C:\My_Folder_Repository" -policy
    "Alta L" -server alta -volume E:\ -date "2008-Sep-20 15:47:35"
    -when after
  ```

  In this example, a snapshot, *E:*, is on *Alta*. This snapshot is mounted to the system where FastBack Mount is running, *X:*. The snapshot is pulled from the network share repository, "*C:\My_Folder_Repository*", by the policy, "*Alta L*". The exact snapshot on the volume to be mounted is the snapshot after *September 20, 2008* at *3:47:35 PM*.

- The following example shows how to mount the most recent snapshot of a volume as a read-only volume, and as a particular user:

  ```
  mount add -login admin -pass admin123 -domain xpress-restore -target
    X: -rep "share:\\snowbird\FB_REP_G user=administrator pass=12345
    domain=my_domain" -policy "Brighton Nighlty" -server Brighton
    -volume E:\ -date "last snapshot" -ro
  ```

  In this example, a snapshot, *E:*, is on the server named *Brighton*. The snapshot is mounted to the system where FastBack Mount is running, *X:*. The snapshot is pulled from the network share repository named "*\\snowbird\FB_REP_G*". *G* is a drive letter for one FastBack repository volume. This share requires a user, password, and domain. This information is supplied in the parameters for **-rep**. In addition, logon credentials are required for FastBack Mount that are provided at the beginning with **-login**, **-pass**, and **-domain**.

del   Use this command type to unmount one or all snapshots from the system where FastBack Mount is running. The following list identifies the tags and parameters for the **del** type:

- **-target** - This tag is required. Use this tag to specify the target to be unmounted. The target to be unmounted can be a virtual volume, reparse point, or iSCSI initiator that was created by using the **mount** command. Use *everything* to unmount all volumes.
- **-force** - Use this tag to force a snapshot to be unmounted. The default option is not to force a snapshot to be unmounted.

For example, to force a snapshot that is mounted at the directory, *c:\gever* to be unmounted, use the following command:

```
mount del -target "c:\gever" -force
```

To unmount a snapshot that is mounted as volume *V:*, use the following command:

```
mount del -target V:
```

To unmount a snapshot that is mounted as an iSCSI initiator, use the following command:

```
mount del -target "ISCSI:<target_name>"
```

dump   Use this type to get a memory dump of all available snapshots in various formats. For example, to dump all snapshots from a network share repository, using a tape format, use the following command:

```
mount dump -type local -rep "C:\My_Folder_Repository" -for
 TapeBackup -full -file "C:\dump.txt"
```

The following list identifies some of the parameters for the **dump** type:

- **-type** - Use **local** for a local repository or **share** for a network-shared repository, or a repository on the folder.
- **-rep** - This tag is required. Use to specify the local or network share repository. For local, you can specify *hostname@domain*, or, for a repository on folder, the full path.
- **-os** - Use this tag to specify the operating system. The options are *windows*, *linux*, and *all*. The default option is *windows*.
- **-for** - Use this tag and the **TapeBackup** parameter to dump each snapshot as an Administrative Command Line command.
- **-full** - Use this tag to carry out a memory dump of all snapshots of each volume. This tag is optional.

  If **-full** is not specified, only the last snapshot of each volume is dumped.
- **-file** - Use this tag to identify a file name to store the memory dump text. This tag is optional.

  If **-file** is not specified, the memory dump text is only printed to **stdout**.

In the following example, you can dump a full list of snapshots that can be mounted from the local repository, in the terminal:

```
mount dump -type local -full
```

```
-----------------------------------------------------------------
SNOWBIRD@OFFICE Alta J     alta     J:\  Last snapshot
SNOWBIRD@OFFICE Alta J     alta     J:\  2009-Aug-22 20:01:49
```

```
SNOWBIRD@OFFICE Snowbird K  snowbird  K:\  Last snapshot
SNOWBIRD@OFFICE Snowbird K  snowbird  K:\  2009-Aug-22 20:24:11
 ----------------------------------------------------------------
```

remove

> Use this type to remove the connection to a non-local repository. There is only one tag for the **remove** type:

> - **-rep** - This tag is required. Use this tag to specify the repository. Connections to this repository are removed.

In the following example, remove all network share repository connections to a repository at "*C:\My_Folder_Repository*":

```
mount remove -rep "C:\My_Folder_Repository"
```

view   Use this type to view a list of all mounted snapshots. This type has no tags. The following example uses the **view** type:

```
mount view
```

```
 ----------------------------------------------------------------
 The following virtual volumes exist:
 'Y:\' is mount of [snowbird@fbperf]-['AltBriPar I LAN'-'alta'-
  'I:\' at 8/22/2009 8:54:42 PM]
 'W:\' is mount of [snowbird@fbperf]-['AltBriPar I LAN'-
  'brighton'-'I:\' at 8/22/2009 8:54:42 PM]
 'V:\' is mount of [snowbird@fbperf]-['AltBriPar I LAN'-
  'parkcity'- 'I:\' at 8/22/2009 8:54:42 PM]
 ----------------------------------------------------------------
```

The following syntax diagram is for the **mount** command:

```
►►—mount—add—[-target]—┬—<virtual_volume>—┬——————————————————————►
                       └—<reparse_point>—┘

►—[-rep]——┬—<hostname@domain>—————————————————————————————————————┬—►
          └—'-"<network_share> user=<username> pass=<password> domain=<domain>"-'—┘

►—[-policy]——<policy_name>——[-server]——┬—<server_name>——┬—————————►
                                       └—'-SAN_layout'—┘

►—[-volume]—┬—<volume>————————┬—[-date]—┬—<date>———————┬—.[-when]—exact—►
            └—<reparse_point>—┘         └—last snapshot—┘

►—[-when]——┬—exact——┬—————————————————————————————————————————————►
           ├—after—┤
           └—before—┘

►—[-login]——<user_name>——[-domain]——<domain>——[-pass]——<password>—┬—[-ro]—┬—►◄
                                                                 └—[-fw]—┘
```
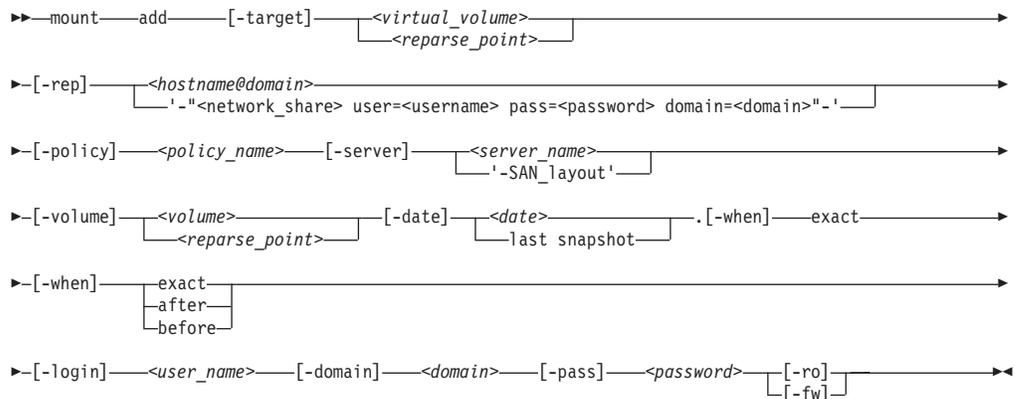
net

Use the **net** command to view network parameters configuration.

Use the following format for the **net** command:

```
net view
```

pjob

Use the **pjob** command to view the list of pending jobs.

Use the following format for the **pjob** command:

```
pjob view number_of_jobs
```

The *number_of_jobs* is the number of pending jobs that is displayed. The default value is *10*. The maximum value is *1000*. The following example identifies how to view the next five pending jobs:

```
pjob view 5
```

For this command to work, the pending job must be in the queue. If there are no jobs in the queue, the jobs are not displayed.

policy

The **policy** command can help you to administer policy operations.

Use the following format for the **policy** command:

```
policy Command_Type -Command_Tag Command_Tag_Parameter
```

The following list summarizes the types that you can specify for the **policy** command. Tags and parameters for each type are listed.

add   Use the **add** command type to add a policy by assigning it a predefined client group and job. The following example indicates the format to use:

```
policy add -pname Command_Tag_Parameter -cname Command_Tag_Parameter
 [-generation Command_Tag_Parameter] [-priority Command_Tag_Parameter]
 [-cname Command_Tag_Parameter]*n -jname Command_Tag_Parameter
 [-jname Command_Tag_Parameter]*n [-enabledr Command_Tag_Parameter]
```

The following list provides detail about the tags and parameters:
- **-pname** - Use to specify the policy name.
- **-generation** - Use to specify the number of generations. A generation is an older version of a snapshot. A generation is not the most recent snapshot.
- **-priority** - Use to set the policy priority. There are three parameters you can use: **h** for high, **m** for medium, and **l** for low.
- **-cname** - Use to specify the client group name.
- **-jname** - Use to specify the backup job name.
- **-enabledr** - Use to enable DR. There are two parameters you can use: **y** for yes and **n** for no.

The following example shows you how to use the tags and parameters with the **add** type:

```
policy add -pname Policy1 -generation 60 -priority h -cname clientG1
 -jname Job1 -jname Job2
```

del   Use the **del** command type to delete an existing policy. The valid command tags are **-pname** and **-all**. The **-cname** command tag indicates the client group name. The **-all** command tag indicates the command runs on all existing policies. For the **-all** command tag, specify *y* for yes or *n* for no as the command tag parameter. The following example indicates the format to use:

```
policy del [-pname command_tag_parameter] [-all command_tag_parameter]
```

edit   Use the **edit** command type to edit an existing policy. The following example indicates the format to use:

```
policy edit -pname Command_Tag_Parameter -rename Command_Tag_Parameter
 [-generation Command_Tag_Parameter] [-priority Command_Tag_Parameter]
 [-cname Command_Tag_Parameter]*n [-jname Command_Tag_Parameter]*n
```

The following list provides detail about the tags and parameters:

- **pname** - Use to specify the policy name.
- **rename** - Use to specify a new name for the policy.
- **generation** - Use to specify the number of generations. A generation is an older version of a snapshot. A generation is not the most recent snapshot.
- **priority** - Use to set the policy priority. There are three parameters you can use: **h** for high, **m** for medium, and **l** for low.
- **cname** - Use to specify the client group name.
- **jname** - Use to specify the backup job name.

The following code sample is an example of how to run the command with the **edit** type:

```
policy edit -pname Policy1 -jname Job1 -jname Job2 -cname "F on winxp-2"
```

info Use the **info** command type to access policy status. The valid command tags are **-pname** and **-request**. The **-pname** command tag indicates the policy name. The **-request** command tag checks to see if a specified job exists. The following examples indicate the format to use:

```
policy info -pname command_tag_parameter -request command_tag_parameter
client_group info -jname "C and D" -request exist
```

view Use the **view** command type to view a list of policies. For example:

```
policy view
```

pause Use the **pause** command type to pause an existing policy. For example:

```
policy pause [-pname command_tag_parameter] [-all command_tag_parameter]
 [-resume command_tag_parameter] [-abort command_tag_parameter]
```

The following list provides detail about the tags and parameters:
- **pname** - Use to specify the policy name.
- **all** - Use to run a command on all existing policies. There are two parameters you can use: **y** for yes and **n** for no.
- **resume** - Use to resume a paused policy. There are two parameters you can use: **y** for yes and **n** for no.
- **abort** - Abort all running jobs of the paused policy. There are two parameters you can use: **y** for yes and **n** for no.

run_now

Use the **run_now** command type to start snapshots on all volumes of a policy. For example:

```
policy run_now [-pname command_tag_parameter] [-type command_tag_parameter]
```

The following list provides detail about the tags and parameters:
- **pname** - Use to specify the policy name.
- **type** - Use to specify the type of snapshot. The first time you take a snapshot, this parameter is not required. For subsequent snapshots, this parameter is required.

(Linux only) For FastBack Clients, the command succeeds when sending the request for snapshot creation reaches the FastBack Server. To see if the snapshot is created, check FastBack Manager.

repository

You can use the **repository** command to view the total and used repository space.

Use the following command for the **repository** command:
```
repository view
```

server

You can use the **server** command to view the version of the FastBack Server.

Use the following command for the **server** command:
```
server view
```

set_connection

The **set_connection** command sets the connection configuration.

Use the following format for the **set_connection** command:
```
set_connection Command_Tag <hostname or IP address>
```

If the FastBack Server cannot connect to the Administrative Command Line, you can manually set the FastBack Server name at the configuration file by running the following command:
```
FastBackShell.exe -c set_connection server_computer FB_SERVER_NAME
```

The following tags can be used with the **set_connection** command:
- **server_computer** - Use to set the FastBack Server connection.
- **mount_computer** - Use to set the FastBack Mount connection.

The following sample sets the Administrative Command Line to work with FastBack Server that uses the *155.155.155.155* IP address:
```
set_connection server_computer 155.155.155.155
```

In the following sample, the Administrative Command Line is set to work with FastBack Mount on the *ComputerName* host.
```
set_connection mount_computer ComputerName
```

snapshot

The **snapshot** command monitors jobs and manages snapshots.

The following command types can be used for the **snapshot** command:
- **del** - Use to delete a specified snapshot. For example, you can use the following command:
  ```
  snapshot del (-rid command_tag_parameter | -rdesc
   command_tag_parameter) -type action_type
  ```

  The following list provides details about tags and parameters:
  - **rid** - The snapshot ID.
  - **rdesc** - The snapshot description.
  - **type** - There are two parameters for **type**: **VIEW_TYPE** and **ACTION_TYPE**. For the **VIEW_TYPE** parameter, the options are *running*, *history*, *info*, and *events*. Use *running* to view snapshots that are running. Use *history* to view snapshots that exist. Use *info* to view information for specific snapshots. Use *events* to view

events for running snapshots. For the `ACTION_TYPE` parameter, the options are *info* and *force*. Use *info* to get information and not run any action. Use *force* to implement the action and ignore any warnings that are displayed.

(Linux only) For FastBack Clients, the command succeeds when sending the request for deletion reaches the FastBack Server. To see whether the snapshot is deleted, check FastBack Manager.

- **view** - Use this type to view a list of jobs that are running. You can use the following example when running the command:

```
snapshot view type view_type [-rid
 command_tag_parameter | -rdesc command_tag_parameter]
```

To view a history of all jobs that completed, you can use the following command:

```
snapshot view -type history
```

The following list provides details about tags and parameters:
  - **rid** - The snapshot ID.
  - **rdesc** - The snapshot description.
  - **type** - There are two parameters for **type**: `VIEW_TYPE` and `ACTION_TYPE`. For the `VIEW_TYPE` parameter, the options are *running*, *history*, *info*, and *events*. Use *running* to view snapshots that are running. Use *history* to view snapshots that completed. Use *info* to view information for specific snapshots. Use *events* to view events for running snapshots. For the `ACTION_TYPE` parameter, the options are *info* and *force*. Use *info* to get information and not run any action. Use *force* to implement the action and ignore any warnings that are displayed.
- **restore** - Use this type to restore a snapshot to a specified volume. You can use the following example when running the command:

```
snapshot restore (-rid P | -rdesc P) -agent P
-restoreType P [-cdpSeconds P] [-cdpTime P] [-force P]
```

The *P* represents the *command_tag_parameter*.The following list provides details about tags and parameters:
  - **agent** - The volume description. The following code sample provides the correct volume description format:

```
server@volume
```

  For example:

```
winxp_station@c:
```

  - **cdpSeconds** - The number of seconds from the following time:

```
1/1/1970 00:00:00
```

  For example, cdpSeconds=1 indicates the following timestamp: 1/1/1970 00:00:01. cdpSeconds=60 indicates the following timestamp: 1/1/1970 00:01:00.This type cannot be used with **cdpTime**.
  - **cdpTime** - This type cannot be used with **cdpSeconds**. The following sample provides the format:

```
mm_dd_yyyy_hh_min_sec
```

  mm is the month. Options are *1* through *12*. *dd* is the day. Options are *1* through *31*. *yyyy* is the year. For example, *2009*. *hh* is the hour. Options are *0* through *23*. *min* is the minutes. Options are *0* through *59*. *sec* is the seconds. Options are *0* through *59*. For example:

```
05_10_2006_15_10_00
```

- **force** - The options are *y*, for *yes*, and *n*, for *no*. Specify *y* to ignore open handles during a restore.
- **rdesc** - The snapshot description.
- **restoreType** - Use this type to specify the type of snapshot to restore. The following options are valid: *full*, *incremental*, and *incremental-last*.
- **rid** - The snapshot ID.

util

The **util** command is used for utilities operations.

The following format should be used for the **util** command:

```
util <command_type> command_tag_parameter
```

The following command types can be used for the **util** command:

- **view** - Use to view **util** parameters. There are three parameters: **time**, **log_level**, and **IP**. For example, you can use the following command:

```
util view (time | log_level)
```

  The **log_level** options are *none*, *errors*, *warnings*, and *all*.

- **exec** - Use to reset the FastBack Server. For example, you can use the following command:

```
util exec reset_xpress_server
```

- **set** - Use to set **util** parameters. There are two parameters: **time** and **log_level**. The **log_level** options are *none*, *errors*, *warnings*, and *all*. You can use the following examples when running the **util** command with these options:

```
util set log_level warnings
util set time 09-20-2008 17:30:25 reset_xpress_server
```

ver

You can use the **ver** command to view versions.

Use the following command for the **ver** command:

```
ver view
```

Administrative Command Line return codes

Return codes help identify the results of Administrative Command Line operations.

Use these return codes to check the status of your Administrative Command Line operations.

Table 32. Administrative Command Line return codes

Return Code	Value
0	FBC_MSG_MOUNT_SUCCESS
1	FBC_MSG_MOUNT_FAIL
2	FBC_MSG_MOUNT_DRIVER_ERROR
3	FBC_MSG_VOLUME_LETTER_BUSY
4	FBC_MSG_MOUNT_WRONG_PARAMETERS
5	FBC_MSG_MOUNT_ALREADY_MOUNTED

Table 32. Administrative Command Line return codes (continued)

Return Code	Value
6	FBC_MSG_MOUNT_WRONG_PERMISSIONS
7	FBC_MSG_MOUNT_NETWORK_DRIVE
8	FBC_MSG_MOUNT_LOCKED_BY_SERVER
9	FBC_MSG_CAN_NOT_CHANGE_REPOSITORY
10	FBC_MSG_DISMOUNT_SUCCESS
11	FBC_MSG_DISMOUNT_FAIL
12	FBC_MSG_VIEW_SUCCESS
13	FBC_MSG_VIEW_FAIL
14	FBC_MSG_DUMP_SUCCESS
15	FBC_MSG_DUMP_FAIL
16	FBC_MSG_CONNECTION_FAILED
17	FBC_MSG_CONNECTION_TIMEOUT
18	FBC_MSG_MOUNT_FAILED_TO_FIND_REPOSITORY
19	FBC_MSG_MOUNT_JOB_NOT_FOUND
20	FBC_MSG_MOUNT_JOB_FOLDER_NOT_FOUND
21	FBC_MSG_MOUNT_WAIT_FOR_NEXT_DR
22	FBC_MSG_CAN_NOT_REMOVE_REPOSITORY
23	FBC_MSG_REPOSITORY_GOT_MOUNTS
24	FBC_MSG_REMOVE_SUCCESS
25	FBC_MSG_IRESTORE_SUBMIT_SUCCESS
26	FBC_MSG_IRESTORE_SUBMIT_FAIL
27	FBC_MSG_IRESTORE_FAILED_TO_FIND_REPOSITORY
28	FBC_MSG_IRESTORE_JOB_NOT_FOUND
29	FBC_MSG_IRESTORE_JOB_FOLDER_NOT_FOUND
30	FBC_MSG_IRESTORE_WAIT_FOR_NEXT_DR
31	FBC_MSG_IRESTORE_WRONG_PARAMETERS
32	FBC_MSG_IRESTORE_WRONG_PPERMISSIONS
33	FBC_MSG_IRESTORE_NETWORK_DRIVE
34	FBC_MSG_IRESTORE_LOCKED_BY_SERVER
35	FBC_MSG_IRESTORE_VOLUME_LETTER_IN_USE
36	FBC_MSG_IRESTORE_ALREADY_RESTORED

Chapter 11. Best practices

There are best practices for Oracle consistent backup and SQL server with named instances backup. The following sections contain details about the best practices.

Tivoli Storage Manager backup-archive client integration

While Tivoli Storage Manager FastBack backs up and restores data, you need to archive protected server data for long-term storage and disaster recovery. IBM Tivoli Storage Manager backup-archive client version 6.1 for Windows includes a configuration wizard that you can use to configure the Tivoli Storage Manager backup-archive client to protect FastBack Client data for long-term storage and disaster recovery.

About this task

The wizard is available as a remote application that uses the web client and as a local application. You can use the wizard to schedule when to store FastBack Client data in the Tivoli Storage Manager server.

The Tivoli Storage Manager Configuration wizard for FastBack is supported on systems that run with the following operating systems: Microsoft Windows XP 32 bit or Microsoft Windows Server 2003 32 bit.

To use the wizard, the Tivoli Storage Manager backup-archive client needs to be installed on the same system where the FastBack Server exists. If a FastBack Disaster Recovery Hub is deployed, the Tivoli Storage Manager backup-archive client needs to be installed on the system with the FastBack Disaster Recovery Hub server. There is no order required for the installation processes. When the Tivoli Storage Manager Configuration wizard starts, the software checks for either a FastBack Server or a FastBack Disaster Recovery Hub server. If either server is not available on the system, the wizard is not usable.

The Configuration wizard for FastBack requires that the Tivoli Storage Manager client is properly configured with a Tivoli Storage Manager server. In addition, the Tivoli Storage Manager client acceptor service, **dsmcad**, must be running. This setup task can be completed by locally running the Tivoli Storage Manager GUI configuration wizard after installing the Tivoli Storage Manager backup-archive client.

The FastBack Server or FastBack Disaster Recovery Hub server is to be installed and configured for short-term data retention before running the Tivoli Storage Manager Configuration wizard for FastBack. In addition, FastBack policies, clients, and volumes are to already be defined in the FastBack Server and at least one snapshot is to be taken.

After you install the software, a post-installation task must be completed. You must specify a FastBack user name and password with administrator authority to be used by the Tivoli Storage Manager Configuration wizard. The wizard uses the user name and password to query and mount volumes from the FastBack Server or to run Tivoli Storage Manager Scheduler scripts.

To configure the user name and password, run the following command on the system where the Tivoli Storage Manager backup-archive client and FastBack Server or FastBack Disaster Recovery Hub server are installed:

```
FastBackShell -c encrypt -u $(username) -d $(domain) -p $(password)
-f <system_drive>\FastbackTSMScripts\credential.txt
```

The `credential.txt` file cannot be changed. The `credential.txt` file must be stored in the `FastbackTSMScripts` directory of the system's system drive for the wizard to run properly.

To start the Configuration wizard from the Tivoli Storage Manager backup-archive client GUI, complete the following steps:

1. Select **Utilities** > **Setup Wizard**. The welcome page for the wizard is displayed.
2. Select **Help me configure the client to protect FastBack Client data**.
3. Click **Next**.
4. To complete the configuration process, use the help provided with the wizard.

If you do not see the **Help me configure the client to protect FastBack Client data** option, the Tivoli Storage Manager backup-archive client is not installed on the same system with FastBack Server or FastBack Disaster Recovery Hub server.

To start the wizard from the Tivoli Storage Manager Web client, complete the following steps:

Procedure

1. Select **Utilities** > **Setup Wizard**.
2. Click **Next**.
3. To complete the configuration process, use the help provided with the wizard.

What to do next

If you do not see the **Setup Wizard** menu displayed, the Tivoli Storage Manager backup-archive client is not installed on the same system with FastBack Server or FastBack Disaster Recovery Hub server.

For information about the Tivoli Storage Manager Client Configuration Wizard for FastBack, see http://www.ibm.com/support/docview.wss?uid=swg21378128.

Integrating FastBack Mount and IBM Tivoli Storage Manager

You can integrate FastBack Mount with IBM Tivoli Storage Manager to back up volumes to a Tivoli Storage Manager server. FastBack Mount can mount any volumes that are stored in a FastBack Server repository that can then be backed up using a Tivoli Storage Manager client to a remote Tivoli Storage Manager server.

Before you begin

The Tivoli Storage Manager client `selective` and `incremental` commands can be used to back up files from a mounted volume. Both command function normally on files within the mounted volume. Tivoli Storage Manager, versions 5.2 and later are supported.

Previous knowledge of IBM Tivoli Storage Manager and FastBack Server is required. Tivoli Storage Manager client must be installed in the default `C:\Program Files` path.

Note: Back up to tape is faster when a full cleanup is carried out before the backup is run.

About this task

To configure Tivoli Storage Manager for use with FastBack Mount, install the Tivoli Storage Manager server and client on different systems. The Tivoli Storage Manager client must be installed on a system with Windows 2000 Service Pack 3 or later.

One system is used for mounting volumes, with FastBack Mount, and backing them up to a Tivoli Storage Manager server. This system does not need to be the client where the volume originally came from or the system with the FastBack Server. The system can be either the client, server, or a third system, unrelated to the FastBack Server or FastBack Client environment.

Install FastBack Mount, the Administrative Command Line, and the Tivoli Storage Manager client on the same system. Do not install firewall, anti-virus, or anti-spyware software on this system. When anti-virus and anti-spyware applications run simultaneously with FastBack Mount, there is high processor usage, resulting in snapshot that run slowly or are stopped. In rare cases, running FastBack Mount with anti-virus and anti-spyware applications can also cause a Windows system crash. If a system crash occurs, restart the system. The system starts normally.

During the FastBack Mount and Administrative Command Line installation, when asked for the IP address, type the IP address for the Tivoli Storage Manager client (that is on the same system).

Results

An Active Directory user that is logged on to the Tivoli Storage Manager client system, and has NTFS permissions to the volumes, can back up data with Tivoli Storage Manager. The backups are run from the Tivoli Storage Manager client command-line utility, **dsmc**. You can use the Windows task scheduler to schedule backups. Each backup is for a single volume.

What to do next

To create a backup, complete the following steps:
1. To get information about volumes that are available for tape backup, run the following command on the Tivoli Storage Manager Client system:

   ```
   fastbackshell.exe -c mount dump -type share -rep "\\$serverName\rep
   user=$DomainUser pass=**** domain=$DomainName" -for TapeBackup -file C:\dump.txt
   ```

   where *$serverName*\rep is the path to the repository share and *user=$DomainUser pass=***** is the same credentials that are specified in the **FastBack Mount Access** tab of the FastBack Manager GUI.

   The output from the command is a file that contains information that looks like the following sample:

   ```
   "%dir%FastBackShell.exe" -c mount add -ro -rep "share: \\computer_name\
   folder_path\London-FastBack\repository user=tapeadmin pass=admin123 domain=
   Taurus" -target "c:\ London-FastBack repository\Policy-DC\London-DC\C" -policy
   "Policy-DC" -server "London-DC" -volume "C:\\" -date "last snapshot"
   ```

If there are multiple volumes in the repository, separate lines are created for each volume.

2. Batch scripts are used to mount, back up, and unmount individual volumes. Create a batch file on the Tivoli Storage Manager client system that mounts a volume. This batch file must be placed in a directory that is named after the system where the volume belongs. Name the batch file after the volume it mounts. For example, for a batch script that mounts the *C* volume of the *London-DC* system, create the *mount_volume_C.bat* file in the *C:\Tape_London_DC* directory.

   To help complete this step, use the following code samples:

   ```
   set dir=c:\Program Files\Tivoli\TSM\FastBack\shell\
   ```

   This section is copied from the dump file that was created in the previous step. For example:

   ```
   "%dir%FastBackShell.exe" -c mount add -ro -rep "share: \\computer_name\
   folder_path\London-FastBack\repository user=tapeadmin pass=admin123 domain=
   Taurus" -target "c:\ London-FastBack repository\Policy-DC\London-DC\C" -policy
   "Policy-DC" -server "London-DC" -volume "C:\\" -date "last snapshot"
   IF %ERRORLEVEL% EQU 0 goto end

   :error_end

   echo could not mount

   EXIT 1

   :end

   EXIT /B 0
   ```

   dir contains a full path to `FastBackShell.exe`. You can replace the following folder with a folder where you want to mount the volume:

   ```
   c:\London-FastBack repository\Policy-DC\London-DC\C
   ```

   For example:

   ```
   C:\mount
   ```

   Use a mounted path that provides details about the mounted volume, for example, computer name, and volume letter. If the dump file has more than one command, use only the command with the volume that you want to back up in this particular backup.

3. Run the batch script from the command line to mount the latest snapshot of the volume that is specified by the *-volume* value to the directory specified by the *-target* value. To mount the latest snapshot to a mount point, enter the following command:

   ```
   mount_volume_C.bat
   ```

   The following string is a sample mount point: `c:\ London-FastBack repository\Policy-DC\London-DC\C`

4. Create another batch script that unmounts a volume on the Tivoli Storage Manager client system. This batch file must be placed in a directory that is named after the system where the volume belongs. Name the batch file after the volume it unmounts. For example, for a batch script that unmounts the *C* volume of the *London-DC* system, create the `dismount_volume_C.bat` file in the following directory: `C:\Tape_London_DC`

   To help complete this step, use the following code samples:

```
set dir="c:\Program Files\Tivoli\TSM\FastBack\shell\"
"%dir%FastBackShell.exe" -c mount del -target C c:\ London-FastBack
repository\Policy-DC\London-DC\C  -force
if %errorlevel% EQU 10 goto end
:error_end
echo could not dismount London-DC\C
EXIT 1
:end
EXIT /B 0
```

5. Run the batch script from the command line to unmount the volume that is specified by the *-target* value. If the volume is still mounted, later Tivoli Storage Manager FastBack snapshots of the volume might fail. To unmount the previously mounted snapshot, enter the following command:

   ```
   dismount_volume_C.bat
   ```

   If the volume is mounted, the next backup might fail.

6. Finally, create a third batch script to back up the volume to the Tivoli Storage Manager server. This batch script calls the previous mounting batch script, then calls **dsmc**, Tivoli Storage Manager client command-line interface application, then call the previous dismounting batch script. This batch file must be placed in the same directory as its two dependent batch scripts. In the following example code, *C:\Tape_London_DC* is where this batch file is stored.

   To help complete this step, use the following code samples:

   ```
   call c:\Tape_London_DC\mount_volume_C.bat >> c:\Tape_London_DC\
   pre_volume_c.log 2>&1

   if %errorlevel% equ 1 goto error_end

   cd C:\"Program Files"\Tivoli\TSM\baclient\

   dsmc.exe sel D:\mount\*  -su=yes

   call c:\ Tape_London_DC dismount_volume_C.bat >> c:\Tape_London_DC\
   pst_volume_c.log 2>&1

   goto end

   :error_end

   echo %date% %time% backup London_dc\volume_C  failed >>
   C:\TSM_Errors/error.log

   :end
   ```

7. Create a directory to store the log file that contains backup errors. For example: `C:\TSM_Errors`

Consistent backup of Oracle databases

This section describes how to use external scripts to complete consistent backups of Oracle databases. The following Oracle versions are supported: Oracle9i and Oracle10g.

To avoid database inconsistency, databases and logs are to be backed up at the same time. The logs that you back up are to include control logs and redo logs. When restoring a database, the logs are to be restored from the same point in time.

Prerequisites

Before beginning a backup of the Oracle database, verify that all prerequisites are met.

The following list identifies the prerequisites to complete before backing up the Oracle database:

- Open the Oracle database.
- Verify that the database is in `ARCHIVELOG` mode. If the database is not in `ARCHIVELOG` mode, use one of the following procedures to change to `ARCHIVELOG` mode:
  - For version Oracle9i, complete the following steps:
    1. Back up the database. Backing up the database is a safeguard in case problems occur while trying to change to `ARCHIVELOG` mode.
    2. Use the Enterprise Management console to log on to the Oracle database.
    3. Click **Network** > **Databases** > *Database_Name* > **Instance** > **Configuration** to open the database configuration window.
    4. Go to the Recovery tab.
    5. Select **Archive Log Mode** and click **Apply**.
    6. A Shutdown Options window is displayed. Choose a normal shutdown and click **Apply**.
    7. After the pop-up database window is closed, click **Network** > **Databases** > *Database_Name* > **Instance** > **Configuration** to open the database configuration window.
    8. Go to the General tab.
    9. Click **All Initialization Parameters**.
    10. Set the `log_archive_start` to *true*.
    11. Click **Apply**.

    When the startup is complete, the settings are ready for performing a hot backup.
  - For version Oracle 10g, complete the following steps:
    1. Back up your database. Backing up the database is a safeguard in case problems occur while trying to change to `ARCHIVELOG` mode.
    2. Open Database Control.
    3. Go to **Maintenance** > **Backup/recovery settings** > **Recovery settings**.
    4. Select **Archive Log Mode**.
    5. In the Shutdown Options window, click **Yes** to restart the system.

General guidelines

To implement consistent application-aware snapshots, complete the following steps:

1. Oracle databases are to be switched to backup mode. Switching to backup mode ensures database consistency. To switch to backup mode, use a pre-consistency-point script.
2. After a snapshot is initiated, Oracle databases are to be switched back to normal mode, by using a pre-snapshot script.
3. After the snapshot is complete, create and use a post snapshot script to delete all archived redo log of the database that was backed up.

Customizable Scripts

(Windows only) The following scripts can be customized to implement application consistency:

- `Oracle9i_PreConsistencyPoint.bat` or `Oracle10g_PreConsistencyPoint.bat` - A batch file that switches the Oracle databases to a consistency state, suitable for a hot backup start. Running this batch file also creates a `Recovery_[database name].sql` script.
- `Oracle9i_postConsistencyPoint.bat` or `Oracle10g_PostConsistencyPoint.bat` - A batch file that switches the Oracle databases out of the consistency state.

(Linux only) The following scripts can be customized to implement application consistency:
- `Oracle10g_PreConsistencyPoint.sh` - A shell script that switches the Oracle databases to a consistency state, suitable for a hot backup start. Running this shell script also creates a `Recovery_[database name].sql` script.
- `Oracle10g_PostConsistencyPoint.sh` - A shell script that switches the Oracle databases out of the consistency state.

The `Recovery_[database name].sql` file is used if the database does not open after a backup operation. *[database name]* is the name of your Oracle database. This file is automatically created for every database that is backed up. Use this file when the database tablespaces are in backup mode and the database cannot be opened. The file can also be used after a restore operation, if the database does not start and prompts with a message about tablespaces in need of media recovery.

The following files are not to be changed:
- (Windows only) `Oracle9i_CreatePreConsistencyPointScript.sql`
- `Oracle10g_CreatePreConsistencyPointScript.sql`
- (Windows only) `Oracle9i_CreatePostConsistencyPointScript.sql`
- `Oracle10g_CreatePostConsistencyPointScript.sql`

Create a script that deletes all archived redo logs of the backed up database. Save the script to the following path: `C:\Program Files\Tivoli\TSM\FastBack\client\scripts`.

Preparing the system
About this task

To prepare the system, install FastBack Client on the Oracle server.

FastBack Server setup
About this task

The following list provides instructions for implementing the schedule of consistent snapshots, by using scripts that are provided with Tivoli Storage Manager FastBack and FastBack Manager:

Note: In the file names specified, *XX* stand for the Oracle version: 9i or 10g.

Procedure
1. (Windows only) Based on the existing databases, change the following fields in the `OracleXX_PreConsistencyPoint.bat` and `OracleXX_PostConsistencyPoint.bat` files:
   a. Change the system user name in the field ORACLE_USR at the beginning of the file.

b. Ensure that the Oracle user name you use has *Alter system* and *Alter table spaces* privileges.

c. Change the system user password in the field ORACLE_PWD at the beginning of the file.

d. Change the database path field ORACLE_DB according to your databases settings. For every Oracle database that you have, make sure that a section exists in Oracle*XX*_PreConsistencyPoint.bat and Oracle*XX*_PostConsistencyPoint.bat. For example, add lines to the script to implement the operation on additional databases.

2. (Linux only) Based on the existing databases, change the following fields in the Oracle10g_PreConsistencyPoint.sh and Oracle10g_PostConsistencyPoint.sh files:

a. Change the system user name in the field ORACLE_USR at the beginning of the file.

b. Ensure that the Oracle user name you use has *Alter system* and *Alter table spaces* privileges.

c. Change the system user password in the field OraclePass at the beginning of the file.

d. Change the OracleDbNames array to list all databases to be backed up. For every Oracle database that you have, make sure that a unique array assignment exists. For example, add a second database with a line like OracleDbNames[2]="dbname" In addition, verify that a connection identifier with the same name as the database exists for each database.

3. Define a policy by using FastBack Manager. The policy schedules the backup of the volumes where Oracle databases are on.

4. Go to the Pre or Post Processes tab and complete the following steps:

a. Select **Pre Consistency-Point**. For the script, type Oracle*XX*_PreConsistencyPoint.bat.

b. Select **Pre Snapshot**. For the script, type Oracle*XX*_PostConsistencyPoint.bat.

c. Select **Post Snapshot**. Type the name of the script you wrote to delete all archived redo logs of the backed up database.

d. Click **Apply**.

Testing the backup

The best way to test the usability of backups is to restore them to a separate host and attempt to open the database. Implement media recovery if necessary.

This option requires that you have a separate host available for the restore procedure.

Testing the integrity of the physical data

Get all data file names and implement the physical data structure integrity check that the **DBVERIFY** utility implements on each file.

The **DBVERIFY** utility is an external command-line utility that implements a physical data-structure integrity check on an offline data file.

Use **DBVERIFY** primarily to ensure that a user-managed backup of a data file is valid before it is restored. Use it also as a diagnostic aid when there are data corruption problems.

The name and location of **DBVERIFY** depends on your operating system.

Restoring the Oracle database

To avoid database inconsistency, back up databases and logs at the same time. The logs that you back up are to include control logs and redo logs. When restoring a database, the logs are to also be restored from the same point in time.

To restore the backed up Oracle database, complete the following steps:

1. Shut down the Oracle database.
2. Perform volume restore, by using the Snapshots Monitor tab of FastBack Manager, or use FastBack Mount to implement an instant restore on Oracle database volumes.
3. Start the Oracle database.

Troubleshooting

Problem: After using the `ApplicationConsistency.bat` script file, the Oracle database does not start, prompting a message about tablespaces that need media recovery.

Workaround: Use the `Recovery.sql` script from the SQL*PLUS worksheet.

Running the recovery script
About this task

For an Oracle 10g database, the recovery script is run by the SQL*PLUS editor.

(Windows only) For an Oracle 9i database, the recovery script is run by the Oracle SQL*PLUS worksheet. To run the recovery script for an Oracle 9i database, complete the following steps:

Procedure

1. Open Oracle 9i SQL*PLUS worksheet for the database with the *sysman* credentials.
2. Use the **Worksheet** > **Run Local Script** option to go to the location of the recovery script.
3. From `C:\Program Files\Tivoli\TSM\FastBack\client\scripts`, select the recovery batch file.
4. An alternative method for running the SQL*PLUS editor is to add double quotation marks (") at the start and the end of the path name. For example, you can enter the following command:

   `@"C:\Program Files\Tivoli\TSM\FastBack\client\scripts\`*`RecoveryMYDB.sql`*`"`

SQL server with named instances backup

If you are using an operating system that supports the VSS service, complete volume snapshots by using the VSS service with FastBack Manager. Do not use the instructions that describe how to use external scripts to run a consistent backup of the SQL Server databases.

The information applies to SQL Server 2005, Version 9, SP2 or later. The instructions provided were tested on a SQL Server Enterprise Edition 2005, Version 9, SP 3 database.

The following points relate to Recovery Model support:

- FastBack supports backup using the Simple Recovery Model. If a database is marked as Full Recovery Model, the database is backed up, but the logs are not purged.
- Named instances are not displayed in FastBack Manager.

Consistency point

To initiate application-aware snapshots, complete the following steps:

1. Disable the VSS service. The VSS service must be disabled before running the snapshot.
2. Notify the SQL Server database administrator that a snapshot is going to run.
3. Initiate the snapshot.
4. Notify the SQL Server database administrator that the snapshot is complete.

Pre or Post Processes scripts

The XRSQL.ini file is to be customized to implement application consistency. XRSQL_PreConsistencyPoint.bat runs XRSQL_Snap.exe one time for every database.

SQL_PostConsistencyPoint.bat batch files notify XRSQL_Snap.exe that the snapshot is implemented, and that the SQL Server can continue running normally.

FastBack Server setup

About this task

To schedule consistent snapshots by using scripts for FastBack Server and FastBack Manager, complete the following steps:

Procedure

1. In the XRSQL.ini file, for every database, add another *[databaseN]* section. The section is to include the following lines:

   instance=
   database_name=
2. In the XRSQL.ini file, in all *[databaseN]* sections, for the *instance* field, change the instance name.
3. In the XRSQL.ini file, in all *[databaseN]* sections, for the *database_name* field, change the database name.
4. For each database, add a section. Increment the database number. For example, *database1*, *database2*, and *database3*.
5. Define a policy by using FastBack Manager. The policy schedules the volume backup for the SQL Server databases. (Do not choose the SQL Server icon on the FastBack Manager)
6. Integrating consistency scripts - on the last step of the policy creation wizard, or after the policy was created:
7. Go to the Pre or Post Processes tab and complete the following steps:
   a. Select **Pre Consistency-Point**. For the script, type XRSQL_PreConsistencyPoint.bat.
   b. Select **Pre Snapshot**. For the script, type SQL_PostConsistencyPoint.bat..
   c. Click **Apply**.

What to do next

Master databases are to be the last database frozen. For example,

```
[database1]
instance=
database_name=DB_NIR

[database2]
instance=
database_name=MASTER
```

If a cluster is used, edit the following section:

```
[server]
name=
```

If a cluster is not used, do not edit this section.

Chapter 12. Troubleshooting

This information describes some common problems that you might have with the Tivoli Storage Manager FastBack and provides possible solutions.

Messages

Problem

The cleanup process fails on all volumes. The following message is displayed in the FastBack Log, Windows Application Log:

```
Cleanup cannot be completed since a snapshot of
[Policy: 'yyy' volume: x on server] is locked by
FastBack Mount on []
```

This problem occurs when the Active Directory is configured to exclude the *local system* account from the *Everyone* group. As a result, the FastBack Server does not access the FastBackSync share and assumes that all snapshots are locked.

Solution

Change the FastBack Server service logon account from *local system* to an Active Directory user.

Problem

When you try to access a shared folder over the network, the following message is displayed:

```
FBSG7354E: The specified location is not accessible.
```

Solution

The cause of the problem is that the FastBack Server service does not have permissions to open shared volumes. You can resolve this problem by changing the logon credentials from *Local System* to *Administrator*. To change these logon credentials, complete the following steps:

1. From the Windows Start menu, select **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click to select the FastBack Server service; then, click **Properties**.
3. In the Properties window, go to the Log On tab.
4. In the **Log on as** list, select **This Account**.
5. Enter the administrator account and authenticate with the domain controller.
6. Click **OK**.

Problem

When you try to remove the only repository on the FastBack Server, the following message is displayed:

```
FBSG4161W Snapshots relocation is impossible
```

Solution

You cannot remove a repository volume from the repository space that has only one repository volume defined. To resolve this problem, add another disk or volume to the repository pool before you delete the repository.

Problem

When you start FastBack Manager, the following message is displayed:

```
FBSG7072E FastBack Manager failed to initiate.
Non-English system.
```

Solution

> This message is displayed if Tivoli Storage Manager FastBack, Version 5.5.0 is installed on a non-English system. Install a globalization enabled version of Tivoli Storage Manager FastBack that supports your language.

Problem

> When you right-click a selected snapshot, then, click **Erase** and the following message is displayed:
>
> ```
> FBSS5013W Can't retrieve snapshot information.
> ```

Solution

> This message is displayed if a cleanup or replication process is running. Stop all cleanup and replication processes. Erase the snapshot.

Problem

> During a snapshot, the following message is displayed in FastBack Manager:
>
> ```
> FBSG7223E The operation failed on some or all of the volumes.
> ```

Solution

> The message indicates that the FastBack Client is not connected. From FastBack Manager, select **General Configuration** > **Storage Pool** to see whether the client is connected. If the client is not connected, go to the client system, open the FastBack Client Configurator and type the correct host name or IP address for the FastBack Server.

Problem

> When you try to connect to the FastBack Server, the following message is displayed:
>
> ```
> FBSG5804E Please verify IP/Computer name because of
> connection failure at <FastBack Server host name>
> ```

Solution

> To resolve this problem, complete the following steps:
>
> 1. Verify that the FastBack Server service started. To check status of a service, from the Windows Start menu, go to **Start** > **Control Panel** > **Administrative Tools** > **Services**. In the Services window, make sure that the FastBack Server service is started.
>
> 2. If the FastBack Server service starts, but shuts down soon after it starts, identify and resolve the startup problem. Check the Windows Event Logs by going to **Start** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
>
> 3. Verify that the FastBack Manager is configured to point to the appropriate host name for the FastBack Server. Use the Windows `ping`, `tracert`, and `nslookup` commands from the Windows command line to determine if the FastBack Server host can be contacted by using the name or IP address that is identified in the message.
>
> 4. If there are multiple network adapters on the host where the FastBack Manager is installed, verify that they are configured such that the network, where the FastBack Server host is located, is on the primary network connection for the host. You can check by using the Windows Network Connections window. The Advanced Settings window provides this information.

In addition, identify the network that the FastBack Server is on. In the Advanced Settings window, on the Adapters and Bindings tab, make sure that the network is the first item in the `Connections` list.

5. Save any changes.
6. Restart the FastBack Server.

Problem

In the Windows Event Viewer (Vista/Windows 2008) the following warning message is displayed:

```
Volume Shadow Copy Service warning: ASR writer Error
0x8007001. hr=0x00000000.
```

Solution

You can ignore this message. The message is displayed only when the snapshot starts while there is a mounted snapshot using FastBack Mount at the backed up server. You can avoid the message by dismounting snapshots before you start a new snapshot.

Problem

In the Windows Event Viewer (Vista) the following message is displayed:

```
Unexpected error VSS_E_WRITER_STATUS_NOT_AVAILABLE
An older active writer session state is being overwritten
by a newer session. The most common cause is that the
number of parallel backups has exceeded the maximum
supported limit. hr = 0x80042409
```

Solution

You can ignore this message. The message has no effect on the snapshot.

Problem

You cannot mount the snapshot with FastBack Mount. The following message is displayed:

```
FBSM8014E Repository is locked by FastBack DR or Fastback Server
```

Solution

The problem is caused by a permissions configuration error during the Tivoli Storage Manager FastBack installation process. To correct the problem, complete the following steps:

1. Log on to the FastBack Manager.
2. On the Configuration tab, click **General Configuration**. In the main window, select the **FastBack Mount Access** tab. Note the User and Domain.
3. On the affected system, open Windows Explorer and go to the `FastBackSync` folder. The default folder location is: `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\FastBackSync`

   By default, the `Application Data` folder is a hidden folder.
4. Right-click on the `FastBackSync` folder; then click **Sharing and Security**.
5. In the properties window, go to the Sharing tab.
6. Click **Permissions**.
7. Add the user account that is defined on the FastBack Mount Access tab. Give the account `Read and Change Permissions`.
8. If the *Everyone* account is listed, either remove the *Everyone* account from the Group or user names list or remove all access permissions for the *Everyone* account. The access permissions are under the `Permissions for Everyone` heading.

9. Click **OK** to save the changes.

10. Restart the FastBack Mount service. Remount the volume.

Problem

When you install the FastBack Client, the installation process fails with the following error message:

```
Error 1722. There is a problem with this Windows Installer
package. A program run as part of the setup did not finish
as expected. Contact your support personnel or package vendor.
```

This problem can also be indicated by the following error message:

```
Error code: -2146368420 [0x8011045c]
exit code 112
No messages on com+ errors.
```

Solution

The problem occurs when FastBack Client tries to register **XR_VSS**, but **XR_VSS** was previously registered. **XR_VSS** is the Tivoli Storage Manager FastBack VSS provider. To resolve this problem, complete the following steps:

1. Uninstall FastBack Client.

2. Restart the system.

3. Go to **Control Panel** > **Administrative Tools** > **Component Services**.

4. Go to **Console Root** > **Component Service** > **Computers** > **My Computer** > **COM+ Application**.

5. Select **XR_VSS** and delete it.

6. Reinstall FastBack Client.

7. Restart the system.

Problem

During the FastBack Client installation, the following message is displayed:

```
FBSM8007E Virtual Volume driver not enabled
```

The virtual volume driver is not installed. If you ignore this message, the message is displayed during a mount of a snapshot on the FastBack Client.

Solution

Install the virtual volume driver with the Windows Add Hardware wizard. For instructions about how to use the wizard, see the Microsoft Windows documentation. After you install the virtual volume driver, open FastBack Mount and mount a snapshot.

Problem

When you try to log on to the remote repository share, the logon fails when the user name and password are entered. The following message is displayed:

```
FBSM8026E <sharename> is inaccessible or not a repository
```

Solution

When you enter the credentials to connect to remote share, use the following domain and user name: *DomainName\administrator*

Problem

When you try to take a snapshot of an Exchange volume, the following message is displayed:

```
VSS freeze failed on  <agent name>
```

.

Solution

This problem occurs when you try to take a snapshot of an Exchange volume that contains a database that is not in a reliable state. An example of database in an unhealthy state is a replica database that is not reliable or an active database that is not mounted. Microsoft Exchange does not allow a database to be VSS frozen when it is not in a good state. The Exchange VSS writer fails to quiesce the unhealthy database. This means that a snapshot cannot be taken of that Exchange volume, or any Exchange volume on the same policy.

You can resolve this problem by ensuring that all databases contained on the volume are in a good state.

VSS allows a crash-consistent snapshot to be taken of a volume that contains an unhealthy database by following these steps:

1. Open the `FastBackClient.ini` file
2. Under the [VSS] section, add the following text:

   `DisableVSSExchangeWriters=true`

3. Save and close the file.

When a snapshot is taken of a volume that contains an unhealthy database, the following message is written to the Job event log:

```
Important: Exchange VSS writer on <agent name> failed to Quiesce the
exchange databases. The snapshot will continue without using
the writer, as specified in <agent name> FastBack
client configuration file.
```

FastBack Server

Question

What is the maximum number of generations for a policy?

Answer

Tivoli Storage Manager FastBack can support 1440 generations per policy.

The number of generations affects the FastBack Server repository space requirements because cleanup processes cannot run on any generation of snapshot on a policy until after the maximum number of generations are stored.

Problem

Moving an existing FastBack Server to a different system without losing the configuration settings.

Solution

If you upgrade your FastBack Server or move the FastBack Server to another system, you can use this solution as a general guide for how to move and what files to move to another system.

This information applies to FastBack Servers that are running with accessible data. This information maintains your backup data, repository, policies, and schedules.

1. Shut down the FastBack Server.
2. Remove the FastBack Server from the network.
3. Attach the new server to the network.
4. Start the new server.

5. Move any physical drives that are to be attached to the system that is the new FastBack Server. If you attach a drive or disk array to the FastBack Server after the Tivoli Storage Manager FastBack is installed, use the `diskopen` tool. You use the `diskopen` tool to identify read and write privileges for the FastBack Server. By default, any disk added to the FastBack Server after Tivoli Storage Manager FastBack is installed is read only. For more information about the `diskopen`tool, see "Allowing read/write access to a disk with disk open utility" on page 102

6. Verify that the new FastBack Server meets all hardware and software requisites. For FastBack Server hardware requirements, see "FastBack Server requirements (Windows only)" on page 26. For FastBack Server software requirements, see "Software requirements and prerequisites" on page 33.

7. Install the FastBack Server. For FastBack Server installation instructions, see "Installing FastBack Server (Windows only)" on page 46.

   If you change the network name or IP address for the server, open the FastBack Client Configurator on the client systems. Change the target to the new FastBack Server.

8. Copy the following files from the `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\Server` directory on the old server:
   - `History.txt` and `History.txt.sig` - These files track all snapshots in the repository.
   - `Orabr_Conf.txt` and `Orabr_Conf.txt.sig` - These files track the general configuration. In the `Orabr_Conf.txt` file, you can configure the SMTP sender field. Look for the `SMTP Sender Name` setting, in the `[Heart Beat]` section.
   - `Conf.txt` and `Conf.txt.sig` - These files track the policy and scheduling configurations.
   - `Clog10.sf` - This file includes general log and error messages.

   These files must be stored in the following directories on the new server:
   - `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\Server`
   - `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\FastBack\Server\Mirror`
   - Root directory of each repository volume

9. Start the new FastBack Server. The server does not, by default, know the location of the repository space.

10. Start FastBack Manager. If FastBack Manager starts in limited mode, you cannot go to the next step until you fix the problem. For more information about limited mode, see "Limited mode" on page 185.

11. Go to **Configuration** > **General Configuration** > **Storage Pool** > **Repository Pool**.

12. Right click to select the repository pool; then, click **Claim Repository**. Claim each repository space that you had for the old server.

13. Verify that the data transfer worked by making sure all of your settings are displayed in the Configuration menu.

14. Verify that the policies are displayed in FastBack Manager.

15. Right click to select a policy; then, click **Run Snapshot**. This step verifies that the new server communicates with clients.
16. Go to the Snapshots Monitor tab to verify that the snapshot ran as scheduled.

Problem

On a FastBack Server running on Microsoft Windows 2008, the FastBack Server service might restart and the server log might state that the memory usage exceeds 85%. This might be because the FastBack Server service might calculate the amount of memory incorrectly, as it looks at free physical memory and free page file memory, but it does not look at the cached physical memory.

Solution

Increase the size of the Windows page file.

Administrative Command Line

Problem

When you use the Administrative Command Line, when you run the interactive mode command, an error message is displayed.

Solution

Open a command prompt and run the following command:

```
FastBackShell.exe -i
```

The FBSC6419E message is displayed. The interactive mode is not available. Currently, there is no workaround.

You can enter the following command to see a list of available commands:

```
FastBackShell.exe -h
```

To run the Administrative Command Line from the command line, enter the following command:

```
FastBackShell.exe -c
```

To run the Administrative Command Line from a script file, enter the following command:

```
FastBackShell.exe -s
```

FastBack Mount

Problem

When you try to mount a volume, the mount fails because the correct credentials for the remote repository share are not entered. The following message is displayed:

```
FSBM8011E not permitted to mount this job
```

Solution

To mount a snapshot, complete the following steps to log on correctly:

1. From FastBack Mount, the Select repository section, click **Remove**.
2. From the Select repository list, select **Browse for Folder**.
3. Select a remote repository share.
4. Enter the user name and password. The user name must be *domain\username*.

Problem

The FastBack Mount icon is not displayed in the Windows System Tray

when you use the Windows Remote Desktop Connection. The Windows Remote Desktop Connection is also known as the Microsoft Terminal Service Client (`mstsc.exe`).

Solution

The problem occurs when the Windows Remote Desktop Connection or Microsoft Terminal Service Client is used without the **/admin** or **/console** switches. To determine which switch to use, open a Windows command line and enter the following command:

```
mstsc.exe /?
```

Either the **/admin** or **/console** switch is displayed. Use the displayed switch when you start sessions on the system. The following examples provide syntax for both options:

```
mstsc.exe /v:system.domain.com /admin
mstsc.exe /v:system.domain.com /console
```

The user that logs on using the **/admin** or **/console** switches must be a member of the Administrator Group on the target system.

Problem

After a backup, a restore file or folder inherits permissions from the parent folder, rather than the original permissions associated with the file. If you use Windows Explorer to drag a file or folder from an image that is mounted with FastBack Mount to a target folder, the original security permissions of the object are not restored. The file or folder inherits permissions from the folder it is copied to.

Solution

To restore a file or folder from a mounted image with the original permissions, use the Windows command-line tool, **XCOPY**, to restore data. For more information about using the **XCOPY** command, see the Microsoft documentation.

Problem

Continuous Data Protection in unavailable with FastBack Mount and instant restore.

Solution

FastBack Mount and instant restore use incremental snapshots. Continuous Data Protection cannot work with incremental snapshots because Continuous Data Protection restores an entire volume to a single point in time that is based on the writes to the volume at a particular point in time. Snapshots with Continuous Data Protection must be restored by the Snapshot Monitor in FastBack Manager.

Problem

How can I use the Read Ahead and Read Ahead Cache Size options in FastBack Mount to improve performance?

Solution

When an application requests data from FastBack Mount, FastBack Mount reads larger chunks of data from the repository to improve performance. The Read ahead option is the amount of extra data that FastBack Mount reads from the repository in addition to the amount of data that is requested by the application. The extra data is held in the Read Ahead Cache. Increasing the size helps when reading and restoring large files that

are stored in consecutive locations on the original disk. It harms performance when it works with small files that are fragmented on the original disk.

The following options can be configured in the general configuration section of the `FastBackMount.conf` file. The last two parameters are used when the data (repository) is stored in a Tivoli Storage Manager server:

- Read Ahead
- Read Ahead Cache Size NTFS
- TSM Read ahead
- Read Ahead Cache Size TSM

The limitations are:

- Read Ahead limit is 4096 16-KB blocks.
- Read Ahead Cache Size NTFS limit is 75000.
- TSM Read ahead limit is 4096 16-KB blocks.
- Read Ahead Cache Size TSM is 75000.

The defaults are:

- Read Ahead = 2
- Read Ahead Cache Size NTFS = 1000
- TSM Read ahead = 64
- Read Ahead Cache Size TSM = 10000

Problem

A problem might arise when FastBack Mount crashes and never restarts (for example, when the system that runs Mount is destroyed). The information about the snapshots what were mounted when FastBack Mount crashed are stored in `xmdrlocks.txt`. The information about these snapshots is never deleted from `xmdrlocks.txt` because FastBack Mount has not unmounted the snapshots, as it crashes and does not restart.

When there are many snapshots that are listed in the `xmdrlocks.txt` file, it takes a long time for the FastBack Server to scan all those snapshots when it tries to unlock and delete them. This operation might cause a remove policy failure. The following message is displayed:

```
The operation could not be performed successfully.
```

.

Solution

The locks in the `xmdrlocks.txt` file remain forever. They are to be manually removed by using one of the following methods.

Method 1: Use this method if you know the host name for the destroyed FastBack Mount machine. In this example, we use "test-machine" as the host name for the destroyed FastBack Mount machine.

1. Open the `xmdrlocks.txt` file. It is in the FastBackSync directory under FastBack installation directory (`..\Tivoli\TSM\FastBack\FastBackSync`).

2. Look for the following information in the file `xmdrlocks.txt`:

```
[XpressMounts]
test-machine_keep_alive = 126
000000027c378c36 = 1
Jobs @
test-machine_000000027c378c36
```

3. Get the ChainID that is to be unlocked. In this example, the chain ID for test-machine is:

```
"000000027c378c36"
```

4. Remove all the information corresponding to "test-machine" and the ChainID under the [XpressMounts] section. In this example, the following records are to be removed:

```
test-machine_keep_alive = 126
000000027c378c36 = 1
test-machine_000000027c378c36
```

5. In the FastBack Manager snapshot monitor panel, check that the locked snapshots can be deleted automatically.

Method 2: Use this method if you do not know the host name for the destroyed FastBack Mount machine.

1. Unmount all snapshots that are mounted by FastBack Mount from a local or remote system.

2. Open the xmdrlocks.txt file. It is in the FastBackSync directory under FastBack installation directory (..\Tivoli\TSM\FastBack\FastBackSync).

3. Get the hostname and ChainID from the section named "Jobs @". In the following example, the host name is test-machine and the ChainID is 000000027c378c36:

```
Jobs @
 test-machine_000000027c378c36
```

4. Remove all the information corresponding to the hostname and the ChainID under the [XpressMounts] section.

5. In the FastBack Manager snapshot monitor panel, check that the locked snapshots can be deleted automatically.

FastBack Manager

Problem

In FastBack Manager, the following message is displayed:

```
The volume configuration of the following Client has changed:
Volume "C:" to "(C:\-Obsolete)" on Client 'filesxsrv'.
Super user should delete and rebuild the affect Client Group if any.
```

In addition, when incremental snapshots run, the following message might be displayed:

```
The operation failed on some or all of the volumes.
Refer to the Server log for details.
Check the Client status and reset the Server.
```

Solution

The message can display for any drive that belongs to any FastBack Client. The message is displayed because the disk signature of one of the volumes changed. The disk signature is calculated with the following values:

- Physical signature
- Size of the partition
- Offset of the partition
- If not in SAN mode, the server name

If any of these values change on the FastBack Client, a new disk signature is calculated. Within seconds of the change, the old disk signature is reported as nonexistent. The other drive with the new disk signature is recognized.

To resolve this problem, complete the following steps:

1. From FastBack Manager, select **General Configuration** > **Client Groups**.

2. Select all groups that are referenced in the message. One of the volumes that you select must be labeled with the following status: *Obsolete*

3. The volume with the *Obsolete* status is the volume with the old disk signature. To update FastBack Client, click the new volume and click **Apply**. The volume with the *Obsolete* status is removed.

For a cluster with the SAN Module enabled, the client group does is not to be marked again.

Problem

FastBack Manager fails during the login process.

Solution

The following list identifies reasons why FastBack Manager does not start, or starts and shuts down:

- The FastBack Server service is not started.
- A message reports that access is denied.

To verify that the FastBack Server service is started, from the Windows Start menu, go to **Start** > **Control Panel** > **Administrative Tools** > **Services**. In the Services window, make sure that the FastBack Server service is started.

To determine whether access is denied, check for access denied messages related to Tivoli Storage Manager FastBack in the Windows Security Event Log.

Problem

In the FastBack Manager Storage Pool window, there are no FastBack Clients displayed. This problem occurs when you use a firewall or add a Network Interface Card (NIC). When you use a firewall or add a NIC, the FastBack Server cannot communicate with or display FastBack Clients in the FastBack Manager Storage Pool window.

Solution

To resolve this problem, complete the following steps:

1. From the Windows Start menu, select **Start** > **All Programs** > **Accessories** > **Communications** > **Network Connections**.

2. From the Advanced menu, select **Advanced Settings**.

3. Go to the Adapters and Bindings tab, in the Connections section, check that the NIC you are using is first on the list.

4. If the NIC is not at the beginning of the list, complete the following steps:

   a. Click **Start** > **Run**.

   b. Type services.msc.

   c. Click **OK**.

   d. Find and stop the FastBack Server and FastBack Watchdog services.

5. In the Adapters and Bindings tab, in the Connections section, select the NIC that the FastBack Server uses and move it as the first item in the list by clicking the arrow to the right of the list.

6. Start the FastBack Server service.

7. Start the FastBack Manager and look at the Storage Pool window. The FastBack Clients is to be displayed.

8. If the FastBack Clients are not displayed, determine whether a firewall is active on the NIC that the FastBack Server is to be using. If the firewall is enabled, ensure that the correct ports are open. For a list of ports that should be open, see "Working with FastBack Manager in WAN environment" on page 89.

FastBack Client

Problem

Continuous Data Protection incremental snapshots and regular incremental snapshots complete successfully, but, in the Snapshots Monitor tab, display *0KB*.

Solution

Except for incremental delta blocks, all snapshots of the FastBack Client complete successfully, but show *0KB* in the size column. Incremental delta blocks that complete successfully display an actual size greater than *0KB*. To resolve the problem, uninstall and reinstall FastBack Client.

Problem

Incremental snapshot backups with FastBack Client process more data than expected and are larger than expected.

Solution

The problem occurs because blocks are changing on the volume that is backed up. The FastBack Client backs up any block-level change that occurs on the volume after the last snapshot backup is taken. This backup includes any changes that are made by temporary or swap-based files, including the following changes:

- Windows temporary folder (for example, `C:\Windows\temp\`)
- Windows virtual paging file (for example, `C:\pagefile.sys`)
- Recycle bin contents (for example, `C:\Recycle Bin\`)
- Hibernation profiles (for example, `C:\hiberfil.sys`)
- System volume cache (for example, `C:\Sysvol`)
- Windows system restore
- Disk defragmentation (for example, Windows defragmentation tool)
- Anti-virus scans (for example, Symantec Anti-Virus)

To minimize the data that is backed up with each snapshot, identify and isolate any applications or Windows configuration that use space on the volume. Try to relocate file or folder locations that are used by these applications to volumes that are not part of the snapshot. In addition, do not disable or enable features that would suddenly delete or create large files, for example, configuring hibernation profiles.

Problem

When a FastBack Client system is rebooted, the next snapshot operation is a delta block snapshot and not an incremental snapshot.

Solution

A delta snapshot occurs (instead of an incremental snapshot) when the FastBack Client system volume is a File Allocation Table (FAT) file system.

Appendix. Accessibility features for the Tivoli Storage Manager product family

Accessibility features help users who have a disability, such as restricted mobility or limited vision to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in the Tivoli Storage Manager family of products:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The Tivoli Storage Manager Information Center and related publications are enabled for accessibility. For information about the accessibility features of the information center, see the following topic: http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/topic/com.ibm.help.ic.doc/iehs36_accessibility.html. Read about the accessibility features of the information center.

Keyboard navigation

On Windows, the Tivoli Storage Manager product family follows Microsoft conventions for all keyboard navigation and access. Drag-and-drop support is managed by using the Microsoft Windows accessibility option known as *MouseKeys*. For more information about MouseKeys and other Windows accessibility options, see the Windows online help, citing the keyword "MouseKeys".

On other operating systems, these products follow the operating-system conventions for keyboard navigation and access.

Vendor software

The Tivoli Storage Manager product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for the accessibility information about its products.

IBM and accessibility

See the IBM Human Ability and Accessibility Center (http://www.ibm.com/able) for information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

Index

A
accessibility features   257
Active Directory
   adding groups   67
   Microsoft Active Directory
      adding groups   67

C
customer support
   contact   xiii

D
databases
   restoring   159
definitions   267
disability   257

E
education
   see Tivoli technical training   xi

F
fixes, obtaining   xii, xiii

G
glossary   267

I
IBM Support Assistant   xii
Internet, search for problem
  resolution   xii
Internet, searching for problem
  resolution   xii

K
keyboard   257
knowledge bases, searching   xii

M
Model database   159
MSDB database
   restoring   159

P
problem determination
   describing problem for IBM Software
     Support   xiv

problem determination *(continued)*
   determining business impact for IBM
     Software Support   xiv
   submitting a problem to IBM
     Software   xv

R
restoring   159
   Model or MSDB databases   159

S
software support
   describing problem for IBM Software
     Support   xiv
   determining business impact for IBM
     Software Support   xiv
   submitting a problem   xv
Software Support
   contact   xiii
support information   xi

T
Tivoli technical training   xi
training, Tivoli technical   xi

U
user accounts
   creating   70
   deleting   71
   properties   70
user groups
   creating   68

Glossary

This glossary includes terms and definitions.

To view glossaries for other IBM products, go to http://www.ibm.com/software/globalization/terminology.

The following cross-references are used in this glossary:

- *See* refers the reader from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- *See also* refers the reader to a related or contrasting term.

A

absolute mode
> In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also *modified mode*.

access control list (ACL)
> In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights. For example, an access control list is associated with a file that identifies the users who can access that file and their access rights.

access mode
> An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume. The access mode can be read/write, read-only, or unavailable. Volumes in primary storage pools can also have an access mode of destroyed. Volumes in copy storage pools can also have an access mode of offsite.

acknowledgment
> The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See *access control list*.

activate
> To validate the contents of a policy set and then make it the active policy set.

active-data pool
> A named set of storage pool volumes that contain only active versions of client backup data.

active file system
> A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. Contrast with *inactive file system*.

active policy set
> The activated policy set that contains the policy rules in use by all client nodes that are assigned to the policy domain. See also *policy domain* and *policy set*.

active version
> The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. Contrast with *inactive version*.

activity log
> A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup
> A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client
> A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the Tivoli Storage Manager server. Contrast with *backup-archive client*.

administrative command schedule
> A database record that describes the planned processing of an administrative command during a specific time period. See also *client schedule*.

administrative privilege class
> See *privilege class*.

administrative session
> A period of time during which an administrator user ID communicates with a server to perform administrative tasks. Contrast with *client node session*.

administrator
> A user who is registered to the server as an administrator, and who is authorized to perform tasks and issue commands through the assignment of an administrative privilege class.

Advanced Program-to-Program Communication (APPC)
> An implementation of the SNA LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

agent node
> A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate
> An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also *logical file* and *physical file*.

aggregate data transfer rate
> A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

APPC See *Advanced Program-to-Program Communication*.

application client
> A program that is installed on a system to protect an application. The Tivoli Storage Manager server provides backup services to an application client.

archive

To copy programs, data, or files to other storage media, usually for long-term storage or security. Contrast with *retrieve*.

archive copy

A file or group of files that was archived to server storage.

archive copy group

A policy object containing attributes that control the generation, destination, and expiration of archived files.

archive-retention grace period

The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also *bind*.

association

(1) The defined relationship between a client node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

(2) On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

audit To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication

The process of checking a user's password before permitting user access to the Tivoli Storage Manager server. Authentication can be turned on or off by an administrator with system privilege.

authentication rule

A specification that another user can use to either restore or retrieve files from storage.

authority

The right to access objects, resources, or functions. See also *privilege class*.

authorization rule

A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user

A user who has administrative authority for the Tivoli Storage Manager client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS

See *automounted file system*.

automatic detection

A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration

The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also *threshold migration* and *demand migration*.

automatic reconciliation

The process that is used to reconcile file systems at regular intervals. The intervals are set by a user with root user authority. See also *reconciliation*.

automounted file system (AutoFS)

A file system that is managed by an automounter daemon. The automounter daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client

A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. Contrast with *administrative client*.

backup copy group

A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class.

backup-retention grace period

The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set

A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection

A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version

A file or directory that a client node backed up to server storage. More than one backup version can exist in server storage, but only one backup version is the active version. See also *active version* and *inactive version*.

bind To associate all versions of a file with a management class name. See *rebind*.

bindery

A database that consists of three system files for a NetWare server. The files contain user IDs and user restrictions.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file

A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See *client acceptor*.

central scheduler
A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See *client schedule* and *administrative command schedule*.

client A software program or computer that requests services from a server.

client acceptor
An HTTP service that serves the applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX, UNIX, and Linux systems, the client acceptor is run as a daemon, and is also called the *client acceptor daemon* (CAD).

client acceptor daemon (CAD)
See *client acceptor*.

client domain
The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node
A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session
A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. Contrast with *administrative session*.

client options file
An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client-polling scheduling mode
A method of operation in which the client queries the server for work. Contrast with *server-prompted scheduling mode*.

client schedule
A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also *administrative command schedule*.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file
A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. This file is also called the dsm.sys file. See also *client user-options file*.

client user-options file
A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also *client system-options file*.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. Contrast with *open registration*.

collocation
The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool. Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group
A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point
A point in time when data is considered consistent.

Common Programming Interface for Communications (CPI-C)
A call-level interface that provides a consistent application programming interface (API) for applications that use program-to-program communications. CPI-C uses LU 6.2 architecture to create a set of interprogram services that can establish and end a conversation, send and receive data, exchange control information, and notify a partner program of errors.

communication method
The method by which a client and server exchange information. See also *Transmission Control Protocol/Internet Protocol*.

communication protocol
A set of defined interfaces that permit computers to communicate with each other.

compression
A function that removes repetitive characters, spaces, or strings of characters from the data being processed and replaces the repetitive characters with control characters. Compression reduces the amount of storage space that is required for the data.

configuration manager
A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also *managed server* and *profile*.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction.

copy backup
A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted

copy group
A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also *archive copy group*, *backup copy group, backup version*, and *management class*.

copy storage pool
A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also *primary storage pool* and *destination*.

CPI-C See *Common Programming Interface for Communications*.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which Tivoli Storage Manager has detected read errors.

data access control mode
A mode that controls whether a command can access a migrated file, see a migrated file as zero-length, or receive an input/output error if it attempts to access a migrated file. See also *execution mode*.

database backup series
One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series.

database snapshot
A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also *database backup series*. Contrast with *full backup*.

data deduplication
A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server
A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover
A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)
A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

default management class
A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

deduplication
See *data deduplication.*

demand migration
The process that is used to respond to an out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated.

desktop client
The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination
A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated.

device class
A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file
(1) For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

(2) For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.

device driver
A program that provides an interface between a specific device and the application program that uses the device.

disaster recovery manager (DRM)
A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan
A file that is created by the disaster recovery manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and hardware that is used by the server, and the location of recovery media.

domain
A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See *policy domain* or *client domain*.

DRM See *disaster recovery manager*.

DSMAPI
See *data storage-management application-programming interface*.

dynamic serialization
A type of copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive.

E

EA See *extended attribute*.

EB See *exabyte*.

EFS See *Encrypted File System*.

Encrypted File System (EFS)
A file system that uses file system-level encryption.

enterprise configuration
A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also *configuration manager*, *managed server*, *profile*, and *subscription*.

enterprise logging
The process of sending events from a Tivoli Storage Manager server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also *event*.

error log
A data set or file that is used to record error information about a product or system.

estimated capacity
The available space, in megabytes, of a storage pool.

event (1) An administrative command or a client operation that is scheduled to be run using Tivoli Storage Manager scheduling.

(2) A message that an Tivoli Storage Manager server or client issues. Messages can be logged using Tivoli Storage Manager event logging.

event record
A database record that describes actual status and results for events.

event server
A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)
For processor storage, real and virtual storage, and channel volume, 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude
The process of identifying files in an include-exclude list. This process

prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup and space management, backup only, or space management only.

exclude-include list

See *include-exclude list*.

execution mode

A mode that controls the space-management related behavior of commands that run under the **dsmmode** command.

expiration

The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file

A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend

To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)

Names or value pairs that are associated with files or directories. There are three classes of extended attributes: user attributes, system attributes, and trusted attributes.

extent The part of a file that is created during the data-deduplication process. Extents are compared with other file extents to identify duplicates.

external library

A type of library that is provided by Tivoli Storage Manager that permits LAN-free data movement for StorageTek libraries that are managed by Automated Cartridge System Library Software (ACSLS). To activate this function, the Tivoli Storage Manager library type must be EXTERNAL.

F

file access time

On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age

For migration prioritization purposes, the number of days since a file was last accessed.

file device type

A device type that specifies the use of sequential access files on disk storage as volumes.

file server

A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space

A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore,

retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)
> A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state
> The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also *resident file*, *premigrated file*, and *migrated file*.

file system migrator (FSM)
> A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state
> The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency
> A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See *file space ID*.

FSM See *file system migrator*.

full backup
> The process of backing up the entire server database. A full backup begins a new database backup series. See also *database backup series* and *incremental backup*. Contrast with *database snapshot*.

fuzzy backup
> A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy
> A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified. See also *backup version* and *archive copy*.

G

General Parallel File System
> A high-performance shared-disk file system that can provide data access from nodes in a cluster environment.

gigabyte (GB)
> In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

global inactive state
> The state of all file systems to which space management has been added when space management is globally deactivated for a client node. When

space management is globally deactivated, hierarchical storage management (HSM) cannot perform migration, recall, or reconciliation. However, a root user can update space management settings and add space management to additional file systems. Users can access resident and premigrated files.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system.

GPFS™
See *General Parallel File System*.

GPFS node set
A mounted, defined group of GPFS file systems.

group backup
The backup of a group containing a list of files from one or more file space origins.

GUID See *Globally Unique Identifier*.

H

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity.

hierarchical storage management (HSM) client
A client program that works with the Tivoli Storage Manager server to provide hierarchical storage management (HSM) for a system. See also *hierarchical storage management* and *space manager client*.

HSM See *hierarchical storage management*.

HSM client
See *hierarchical storage management client*.

I

ILM See *information lifecycle management*.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. Contrast with *active file system*.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. Contrast with *active version*.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also *include-exclude list*.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services.

incremental backup
(1) A copy of all database data that has changed since the most recent successful full backup operation. An incremental backup is also known as a *cumulative backup image* because each incremental backup includes the contents of the previous incremental backup.

(2) The process of backing up information in the database that is new or changed since the last full backup. Contrast with *full backup*. See also *database backup series*.

(3) For Data Protection for Microsoft Exchange Server, a backup in which the transaction logs are backed up and then cleared.

individual mailbox restore
See *mailbox restore*.

information lifecycle management (ILM)
GPFS policy-based file management for storage pools and file sets.

inode The internal structure that describes the individual files on AIX, UNIX, or Linux systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the IP standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 210 or 1 024 bytes. For disk storage capacity and communications volume, 1 000 bytes.

L

LAN See *local area network*.

LAN-free data movement
The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network. This process is also referred to as *LAN-free data transfer*.

LAN-free data transfer
See *LAN-free data movement*.

leader data
Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library
(1) A repository for demountable recorded media, such as magnetic disks and magnetic tapes.

(2) A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client
A server that uses server-to-server communication to access a library that is managed by another storage management server. See also *library manager*.

library manager
A server that controls device operations when multiple storage management servers share a storage device. See also *library client*.

local (1) Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line.

(2) For HSM products, pertaining to the destination of migrated files that are being moved.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volumes
Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See *loopback virtual file system*.

logical file
A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also *aggregate* and *physical file*.

logical occupancy
The space that is used by logical files in a storage pool. This space does

not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy.

logical unit (LU)
An access point through which a user or application program accesses the Systems Network Architecture (SNA) network to communicate with another user or application program.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier that is used to differentiate devices, each of which is a logical unit (LU).

logical volume
A portion of a physical volume that contains a file system.

logical volume backup
A backup of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)
Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)
A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LU   See *logical unit*.

LUN   See *logical unit number*.

LVSA See *Logical Volume Snapshot Agent*.

M

macro file
A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. Contrast with *Tivoli Storage Manager command script*.

mailbox restore
A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object
In Tivoli Storage Manager, a definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server. In general, a managed object cannot be modified locally on the managed server. Objects can include policy, schedules, client option sets, server scripts, administrator registrations, server definitions, and server group definitions.

managed server
A Tivoli Storage Manager server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also *configuration manager*, *subscription*, and *profile*.

management class
A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also *copy group*, *space manager client*, *bind*, and *rebind*.

maximum transmission unit
The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See *megabyte*.

media server
In a z/OS® environment, a program that provides access to z/OS disk and tape storage for Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)
(1) 1 048 576 bytes (2 to the 20th power) when used in this publication.

(2) For processor storage, real and virtual storage, and channel volume, 2 to the power of 20 or 1 048 576 bits. For disk storage capacity and communications volume, 1 000 000 bits.

metadata
Data that describes the characteristics of data; descriptive data.

migrate
To move data from one storage location to another. In Tivoli Storage Manager products, migrating can mean moving data from a client node to server storage, or moving data from one storage pool to the next storage pool defined in the server storage hierarchy. In both cases the movement is controlled by policy, such as thresholds that are set. See also *migration threshold*.

migrated file
A file that has been copied from a local file system to Tivoli Storage Manager storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also *stub file* and *resident file*. For HSM clients on UNIX or Linux systems, contrast with *premigrated file*.

migrate-on-close recall mode
A mode that causes a migrated file to be recalled back to its originating file system temporarily. Contrast with *normal recall mode* and *read-without-recall recall mode*.

migration job
A specification of files to migrate, and actions to perform on the original files after migration. See also *job file*.

migration threshold
High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring
The process of writing the same data to multiple locations at the same time. Mirroring data protects against data loss within the recovery log.

mode A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See *modified mode* and *absolute mode*.

modified mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also *absolute mode*.

mount limit
The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also *mount point*.

mount point
On the Tivoli Storage Manager server, a logical drive through which volumes in a sequential access device class are accessed. For removable-media device types, such as tape, a mount point is a logical drive that is associated with a physical drive. For the file device type, a mount point is a logical drive that is associated with an I/O stream. The number of mount points for a device class is defined by the value of the mount limit attribute for that device class. See also *mount limit*.

mount retention period
The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period
The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See *maximum transmission unit*.

N

Nagle algorithm
An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe
A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS See *network-attached storage*.

NAS node
A client node that is a network-attached storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system
A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format
A format of data that is written to a storage pool directly by the Tivoli Storage Manager server. Contrast with *non-native data format*.

NDMP
> See *Network Data Management Protocol*.

NetBIOS
> See *Network Basic Input/Output System*.

network-attached storage (NAS) file server
> A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System (NetBIOS)
> A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

Network Data Management Protocol (NDMP)
> A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate
> A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

node name
> A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class
> A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also *privilege class*.

non-native data format
> A format of data that is written to a storage pool that differs from the format that the server uses for operations.

normal recall mode
> A mode that causes a migrated file to be copied back to its originating file system when it is accessed.

O

offline volume backup
> A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup
> A backup in which the volume is available to other system applications during the backup operation.

open registration
> A registration process in which users can register their workstations as client nodes with the server. Contrast with *closed registration*.

operator privilege class
> A privilege class that gives an administrator the authority to disable or halt

the server, enable the server, cancel server processes, and manage removable media. See also *privilege class*.

options file
A file that contains processing options. On Windows and NetWare systems, the file is called dsm.opt. On AIX, UNIX, Linux, and Mac OS X systems, the file is called dsm.sys.

originating file system
The file system from which a file was migrated. When a file is recalled using normal or migrate-on-close recall mode, it is always returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the Tivoli Storage Manager server that the client node is contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

out-of-space protection mode
A mode that controls whether the program intercepts out-of-space conditions. See also *execution mode*.

P

pacing
In SNA, a technique by which the receiving system controls the rate of transmission of the sending system to prevent overrun.

packet In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode
A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation
A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting. Password generation can be set in the options file (`passwordaccess` option). See also *options file*.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character
See *wildcard character*.

physical file
A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also *aggregate* and *logical file*.

physical occupancy
The amount of space that is used by physical files in a storage pool. This

space includes the unused space that is created when logical files are deleted from aggregates. See also *physical file*, *logical file*, and *logical occupancy*.

plug-in
> A self-contained software component that modifies (adds, or changes) the function in a particular system. When a plug-in is added to a system, the foundation of the original system remains intact.

policy domain
> A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain.

policy privilege class
> A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also *privilege class*.

policy set
> A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also *active policy set* and *management class*.

premigrated file
> A file that has been copied to Tivoli Storage Manager storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in Tivoli Storage Manager storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. Contrast with *migrated file* and *resident file*.

premigrated files database
> A database that contains information about each file that has been premigrated to Tivoli Storage Manager storage. The database is stored in a hidden directory named `.SpaceMan` in each file system to which space management has been added.

premigration
> The process of copying files that are eligible for migration to Tivoli Storage Manager storage, but leaving the original file intact on the local file system.

premigration percentage
> A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool
> A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also *destination* and *copy storage pool*.

privilege class
> A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also *node privilege class*, *operator privilege class*, *policy privilege class*, *storage privilege class*, and *system privilege class*.

profile
A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also *configuration manager* and *managed server*.

Q

quota (1) For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.

(2) For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization
The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume
A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

read-without-recall recall mode
A mode that causes hierarchical storage management (HSM) to read a migrated file from storage without storing it back on the local file system. The last piece of information read from the file is stored in a buffer in memory on the local file system. Contrast with *normal recall mode* and *migrate-on-close recall mode*.

rebind
To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also *bind*.

recall In Tivoli Storage Manager, to copy a migrated file from server storage back to its originating file system using the space management client. See also *transparent recall*, *selective recall*, and *recall mode*.

recall mode
A mode that is assigned to a migrated file with the **dsmattr** command that determines how the file is processed when it is recalled. It determines whether the file is stored on the local file system, is migrated back to Tivoli Storage Manager storage when it is closed, or is read from Tivoli Storage Manager storage without storing it on the local file system.

receiver
A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the Tivoli Storage Manager server console and activity log. See also *event*.

reclamation
The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold

The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation

The process of synchronizing a file system with the Tivoli Storage Manager server, and then removing old and obsolete objects from the Tivoli Storage Manager server.

recovery log

A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register

To define a client node or administrator ID that can access the server.

registry

A repository that contains access and configuration information for users, systems, and software.

remote

(1) Pertaining to a system, program, or device that is accessed through a communication line.

(2) For HSM products, pertaining to the origin of migrated files that are being moved.

resident file

On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in Tivoli Storage Manager storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from Tivoli Storage Manager storage and modified. Contrast with *stub file* and *premigrated file*. See *migrated file*.

restore

To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention

The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve

To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool.

roll back

To remove changes that were made to database files since the last commit point.

root user

A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See *storage area network*.

schedule
A database record that describes client operations or administrative commands to be processed. See *administrative command schedule* and *client schedule*.

scheduling mode
The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume
A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. Contrast with *Tivoli Storage Manager command script*.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup
The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. Contrast with *incremental backup*.

selective migration
The process of copying user-selected files from a local file system to Tivoli Storage Manager storage and replacing the files with stub files on the local file system. Contrast with *threshold migration* and *demand migration*.

selective recall
The process of copying user-selected files from Tivoli Storage Manager storage to a local file system. Contrast with *transparent recall*.

serialization
The process of handling files that are modified during backup or archive processing. See *dynamic serialization*, *static serialization*, *shared static serialization*, and *shared dynamic serialization*.

server A software program or a computer that provides services to other software programs or other computers.

server options file
A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode
A client/server communication technique where the server contacts the client node when tasks must be done. Contrast with *client-polling scheduling mode*.

server storage
The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from space manager client nodes (space-managed files). See also *active-data pool*, *primary storage pool*, *copy storage pool*, *storage pool volume*, and *volume*.

session

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

session resource usage

The amount of wait time, processor time, and space that is used or retrieved during a client session.

shared dynamic serialization

A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. Tivoli Storage Manager retries the backup or archive operation a number of times; if the file is being modified during each attempt, Tivoli Storage Manager will back up or archive the file on its last try. See also *serialization*. Contrast with *dynamic serialization*, *shared static serialization*, and *static serialization*.

shared library

A library device that is used by multiple storage manager servers.

shared static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. Tivoli Storage Manager attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *static serialization*.

snapshot

An image backup type that consists of a point-in-time view of a volume.

space-managed file

A file that is migrated from a client node by the space manager client. The space manager client recalls the file to the client node on demand.

space management

The process of keeping sufficient free storage space available on a local file system for new data by migrating files to server storage. Synonymous with *hierarchical storage management*.

space manager client

A program that runs on a UNIX or Linux system to manage free space on the local file system by migrating files to server storage. The program can recall the files either automatically or selectively. Also called *hierarchical storage management (HSM) client*.

space monitor daemon

A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file

A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file

On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL   See *Secure Sockets Layer*.

stabilized file space
A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Each stanza is identified by a name that occurs in the first line of the stanza. Depending on the type of file, a stanza is ended by the next occurrence of a stanza name in the file, or by an explicit end-of-stanza marker. A stanza can also be ended by the end of the file.

startup window
A time period during which a schedule must be initiated.

static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the storage manager cannot back up or archive the file. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *shared static serialization*.

storage agent
A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)
A dedicated storage network that is tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
(1) A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also *storage pool*.

(2) An arrangement of storage devices with different speeds and capacities. The levels of the storage hierarchy include: main storage, such as memory and direct-access storage device (DASD) cache; primary storage (DASD containing user-accessible data); migration level 1 (DASD containing data in a space-saving format); and migration level 2 (tape cartridges containing data in a space-saving format).

storage pool
A named set of storage volumes that are the destination that is used to store client data. A storage pool contains backup versions, archive copies, and files that are migrated from space manager client nodes. A primary storage pool is backed up to a copy storage pool. See also *primary storage pool*, *copy storage pool*, and *active-data pool*.

storage pool volume
A volume that has been assigned to a storage pool. See also *volume*, *active-data pool*, *copy storage pool*, and *primary storage pool*.

storage privilege class
A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also *privilege class*.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows

transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file
> A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from Tivoli Storage Manager storage. It also contains additional information that can be used to eliminate the need to recall a migrated file.

stub file size
> The size of a file that replaces the original file on a local file system when the file is migrated to Tivoli Storage Manager storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription
> In a Tivoli environment, the process of identifying the subscribers that the profiles are distributed to. For Tivoli Storage Manager, a subscription is the process by which a managed server receives configuration information associated with a particular profile on a configuration manager. See also *managed server*, *configuration manager*, and *profile*.

system privilege class
> A privilege class that gives an administrator the authority to issue all server commands. See also *privilege class*.

Systems Network Architecture (SNA)
> The description of the logical structure, formats, protocols, and operational sequences for transmitting information through and controlling the configuration and operation of networks.

T

tape library
> A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix
> The high-level-qualifier of the file name or the data set name in the standard tape label.

target node
> A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See *trusted communications agent*.

TCP/IP
> See *Transmission Control Protocol/Internet Protocol*.

threshold migration
> The process of moving files from a local file system to Tivoli Storage Manager storage based on the high and low thresholds that are defined for the file system. Contrast with *demand migration*, *selective migration*, and *migration job*.

throughput
> In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout
> A time interval that is allotted for an event to occur or complete before operation is interrupted.

timestamp control mode
> A mode that determines whether commands preserve the access time for a file or set it to the current time.

Tivoli Storage Manager command script
> A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic.

tombstone object
> A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)
> An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

transparent recall
> The process that is used to automatically recall a file to a workstation or file server when the file is accessed. See also *recall mode*. Contrast with *selective recall*.

trusted communications agent (TCA)
> A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See *Universal Naming Convention name*.

Unicode
> A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus some classical and historical texts. The Unicode standard has a 16-bit character set defined by ISO 10646.

Unicode-enabled file space
> Unicode file space names provide support for multilingual workstations without regard for the current locale.

Unicode transformation format 8
> Unicode Transformation Format (UTF), 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208.

Universal Naming Convention (UNC) name
　　A name that is used to access a drive or directory containing files shared across a network. The UNC name includes the system name and a SharePoint name that represents the shared drive or directory.

Universally Unique Identifier (UUID)
　　The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier.

UTF-8 See *Unicode transformation format 8*.

UUID See *Universally Unique Identifier*.

V

validate
　　To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version
　　A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space
　　A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual volume
　　An archive file on a target server that represents a sequential media volume to a source server.

volume
　　A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also *scratch volume*, and *storage pool volume*.

volume history file
　　A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service
　　A set of Microsoft application-programming interfaces (APIs) that you can use to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See *Volume Shadow Copy Service*.

VSS Backup
　　A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore
　　A function that uses a Microsoft Volume Shadow Copy Service (VSS)

software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on local shadow volumes.

VSS Instant Restore
A volume-level hardware-assisted Microsoft Volume Shadow Copy Service (VSS) function where target volumes that contain the snapshot are copied back to the original source volumes.

VSS offloaded backup
A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W

wildcard character
A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workstation
A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name
A 64-bit, unsigned name identifier that is unique.

workload partition (WPAR)
A partition within a single operating system instance.

IBM ®

Product Number: 5724-U93

Printed in USA