TSM Edition User Guide

Version 8.2

Trademarks and Copyrights

© Copyright Storix, Inc. 1999-2016 USA
Storix is a registered trademark of Storix, Inc. in the USA
SBAdmin is a trademark of Storix, Inc in the USA and other countries
Linux is a registered trademark of Linus Torvalds.
Intel, Pentium, IA32, Itanium, Celeron and IA64 are registered trademarks of Intel Corporation.
AMD, Opteron, and Athlon are registered trademarks of Advanced Micro Devices.
HP Integrity servers are registered trademarks of Hewlett-Packard Development Company
IBM, RS6000, AIX, Tivoli, AIX, pSeries, Micro Channel and RS/6000 Scalable POWERParallel Systems
are registered trademarks of International Business Machines Corporation.
Sun Microsystems and the Solaris™ operating system is a trademark of Sun Microsystems, Inc.
SPARC is a trademark of SPARC International, Inc.
Xwindows is a trademark of Massachusetts Institute of Technology.
Microsoft and Windows are registered trademarks of Microsoft Corporation.
Macintosh and Mac OS X are registered trademarks of Apple Computer, Inc.
All other company/product names and service marks may be trademarks or registered trademarks of their respective companies.

Publicly Available Software

This product either includes or is developed using source code that is publicly available:

AESCrypt*	Rijndael and Cipher Block Feedback mode (CFB-128) encryption/decryption algorithms	Copyright 1999, 2000 Enhanced Software Technologies Inc. http://aescrypt.sourceforge.net/
BusyBox	Single executable containing tiny versions of common UNIX utilities	Copyright 1989, 1991 Free Software Foundation, Inc. http://busybox.net/cgi-bin/cvsweb/busybox/
LILO	LInux boot Loader	Copyright 1999-2003 John Coffman. Copyright 1992-1998 Werner Almesberger. http://freshmeat.net/projects/lilo/
Tcl	Open source scripting language	Copyright Regents of the University of California, Sun Microsystems, Inc. http://tcl.sourceforge.net
Tk	Tk graphics toolkit	Copyright Regents of the University of California, Sun Microsystems, Inc. http://tcl.sourceforge.net
DropBear	A Smallish SSH 2 Server and Client	Copyright 2002, 2003 Matt Johnston http://www.matt.ucc.asn.au/dropbear/dropbear.html
GRUB	Grand Unified Bootloader (GNU GRUB)	Copyright 1989, 1991 Free Software Foundation, Inc. http://www.gnu.org/software/grub/grub.html
Lighttpd	Secure, fast, compliant and flexible web-server	Copyright 2004 Jan Kneschkle, incremental http://www.lighttpd.net
OpenSSL	Toolkit implementing Secure Socket Layer	Copyright 1998-2008 The OpenSSL Project Copyright 1995-1998 Eric A. Young, Tim J. Hudson http://www.openssl.org
Xpdf	PDF Document viewer (for AIX)	Copyright 1996-2003 Glyph & Cog, LLC. http://www.foolabs.com/xpdf
bpgetfile	RPC Bootparams client (for Solaris)	Copyright 2000 Rensselaer Polytechnic Institute, Department of Computer Science
parted	GNU parted	Copyright 2007 Free Software Foundation, Inc. http://www.gnu.org/software/parted
ELILO	Linux boot loader for EFI/x86_64 based systems	Copyright 2000-2003 Hewlett Packard Co. Copyright 2006-2010 Intel Co. ftp://ftp.hpl.hp.com/pub/linux-ia64
btrfs-progs	Btrfs utilities programs	Copyright 2007 Oracle Copyright 2012 STRATO AG http://www.btrfs.wiki.kernel.org

*Encryption Software

System Backup Administrator Backup Data Encryption Feature has a cryptographic component, using ***Advanced Encryption Standard (AES)*** "Rijndael" encryption algorithm in Cipher Block Feedback (stream) mode (CFB-128), supporting 128, 192 and 256-bit keys.

It is not for export or redistribution to any of what are called the "T-10 Terrorist States" as determined by the U.S. Department of State. System Backup Administrator Backup Data Encryption Feature has been registered with U.S. Bureau of Information and Security and is distributed under Export Control Classification Number (ECCN) 5D992. This encryption item is authorized for export and re-export under section 742.15 (B)(2) of the Export Administration Regulations (EAR).

Table of Contents

1. Getting Started

Supported Operating Systems & Hardware

As of the time of this publication, the *TSM Edition* software is supported on all AIX, Solaris, and Linux systems on which the ***TSM Backup/API Client*** software is supported. This includes, but is not necessarily limited to, the following systems:

AIX: All IBM *RS/6000*, *System p*, System i, *OpenPower* and *JS/20* systems running AIX Version 5.1 and later (currently 7.1).

Solaris: **x86 and x86_64**: All Solaris 9 versions 9/05 and later (32 and 64-bit platforms), Solaris 10 versions 1/06 and later (32 and 64-bit platforms), Solaris 11 Express (64-bit platform), and Solaris 11 version 11/11 and later (64-bit platform).

SPARC: All Solaris 9 versions 9/05 and later, Solaris 10 versions 11/06 and later, Solaris 11 Express, and Solaris 11 version 11/11 and later. Includes *sun4u* and *sun4v* platforms.

Linux: ***x86 and x86_64***: All distributions which run on *Intel 32-bit* based processors and 64-bit processors capable of running 32-bit software (includes *AMD*, *Opteron* and *Athlon*-based systems). Linux kernel levels 2.4 and glibc 2.2.5 and higher are required. Support is provided for Linux LVM Library version 1.0 and higher, and Software Raid Devices (meta-disks) when installed. UEFI is supported on x86_64 systems running 2.6.21 or later kernel levels, CONFIG_EFI enabled in the kernel, and support for creating VFAT filesystems.

PPC (IBM system P): All distributions supported 64-bit systems with *PowerPC CHRP* hardware. Linux kernel levels 2.6.16 and higher, and glibc 2.4.2 and higher are required. Support is provided for Linux LVM Library version 1.0 and higher, and Software Raid Devices (meta-disks) when installed.

Software and License Requirements

Installation of the TSM Edition software provides the graphical user interface, web interface and application programs for administering the backups of the *admin system* itself. Administration of client (node) system backups may also be performed from the *admin system*. It is also necessary to install a subset of the software onto each system that will act as either a backup media server or client.

The following table describes license types related to *TSM Edition*:

TSM Edition	This license is installed onto a system from which *TSM (Tivoli Storage Manager)* backups will be managed. This system must be an AIX, Solaris or Linux system and does not need to be a TSM Server. The TSM Edition license supports **Full System Backups** and backups are performed to any TSM server or to a local tape device on each client. Any number of TSM servers may be configured, but you must have a Client License for each additional client (node) to be backed up. This integrates the Full System Backup and Adaptable System Recovery functionality of SBAdmin with the data file storage capabilities of TSM. A single license key is required for the TSM *Admin system*, which also defines the number of TSM clients (nodes) which may be managed by the administrator. Although no license key is requires for each of the clients, the client software must be installed and configured on each TSM node before they may be managed by the TSM Admin system.

TSM Client	Must be installed on each system which will be a client or backup media server. A *Client* license for the local (administrator) system is included with the *TSM Edition* license. This client must be managed by a TSM *Admin system*. No license key is required on the client since the number of supported clients and backup servers are defined by the *TSM Edition* license. Backup management features, such as scheduling and history reporting are provided only by the *TSM Edition*.
Backup Data Encryption Feature	This optional license may be added to a *TSM Edition* license to enable AES data encryption support for all backups. A license is purchased for the number of *Clients* for which backup data should be encrypted.

Other administrator license editions for *Network,* and *Workstation* are also available, which provide backups to local and remote (*Network Edition*) disk and tape devices. Those editions also support multiple backup types, from files and directories to volume groups and raw logical volumes. Since this *TSM Edition* supports only **Full System Backups** and **TSM Servers** as backup media, all other administrator licenses are documented in a separate user guide. Refer to the ***System Backup Administrator User Guide*** for details.

Evaluation License Key

All license options and features above, except the ***TSM Client*** require a license key. The license keys are installed only onto the TSM *Admin system*, and must be obtained from Storix. For all licensed options, the user may type the word "**trial**" for a free 30-day evaluation of all features of the software.

Software Installation and Configuration

The following instructions may be used to install the software from either installation images downloaded from the Storix Software web site (http://www.storix.com) or from a SBAdmin installation CDROM:

Downloading and Installing from the Web Site

1. Select the software package you wish to download from the web site based on your ***operating system type, machine type*** and desired ***software configuration***.

   Be sure to download the file in BINARY. Some browsers will recognize the ".tar" extension of the file and ask you if it should open the file or expand it. You should NOT do so, but select to save it to disk instead.

2. Change to the /tmp directory:

   ```
   cd /tmp
   ```

3. Extract the contents of the file. Note that this does not extract the software, but only the installation program files and install image:

   ```
   tar -xvf IMAGEFILE.tar
   ```
   (where *IMAGEFILE*.tar is the name of the downloaded file)

4. Run the installation program by typing:

   ```
   ./stinstall
   ```

Installing from CDROM

1. Mount the cdrom by typing:

   a. On ***AIX*** systems: **`mount -v cdrfs -r /dev/cd0 /mnt`**

   b. On ***Linux*** systems: **`mount –t iso9660 –r /dev/cdrom /mnt`**

   c. On ***Solaris*** systems: Normally, a CDROM will automatically be mounted to the ***/cdrom/cdrom*** directory when inserted. If this is the case, replace ***/mnt*** with /***cdrom/cdrom*** in the following commands. If the cdrom is not auto-mounted, type:

   `mount -F hsfs –o ro /dev/dsk/c1t0d0s0 /mnt`

   (where c1t1d0s0 is an example of your cdrom drive name).

2. Run the installation program by typing the following, then follow the instructions provided:

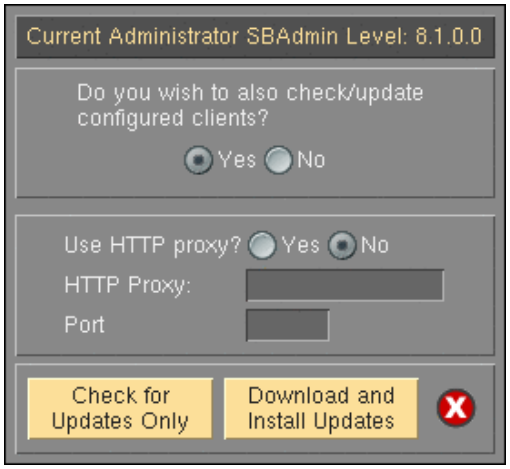
   `/mnt/stinstall`

3. When complete, unmount the CDROM by typing:

   `umount /mnt`

Updating the Software

To update the software connected to the internet, you can automatically check, download and apply updates directly from the Storix Web Server by selecting Help→Download Software Updates from the user interface. A screen similar to the following will appear:



You will have an option of checking for updates only and/or downloading and installing updates. You will have an additional option of automatically applying updates to configured clients.

If the system cannot contact the Storix Web Server directly, you may apply updates by re-installing the software using the same instructions used to initially install the software (shown above). When you re-install the software onto the *Admin system* using the "**stinstall**" command described above, you will be asked if you wish to install the new software level onto configured clients.

> **Re-installing the software will replace existing program files, but WILL NOT OVERWRITE current configuration or history files.**

Starting the Software

There are three user-interfaces available for performing SBAdmin operations:

1. **Graphical-User (Xwindows) interface (GUI)** - This is the interface described in this user guide.

   To access the graphical user interface, also referred as the "***backup administrator***", type:

   ```
   sbadmin
   ```

   from within an *xterm* window. If you wish to run the application on a display attached to a different host (perhaps even a PC running an Xwindows emulator), type:

   ```
   sbadmin –display hostname:0 &
   ```

   (where *hostname* is the host name of the remote system). It may also be necessary to provide access to the application to write to the display by first typing "**`xhost +`**" within an *xterm* window on the remote system.

   When starting the administrator software, the Main Screen will appear.

2. **Web-based interface** – This interface is accessed through a web browser and is designed to be similar in use and function to the GUI interface. You must have enabled the web interface when installing the software on the Administrator System. Refer to the ***SBAdmin Web Interface Install Guide*** for additional details on installing, configuring and starting this interface.

3. **Command-line Interface (CLI)** – This refers to running commands provided with this software at the shell prompt. Commands may only be run when logged on as the root user, or another user already configured using the GUI or Web interface. Various commands may be run on the administrator or client system. Refer to the **SBAdmin Commands Reference** for details.

Enabling Optional Features

The optional feature, ***Backup Data Encryption***, may be enabled after the *TSM Edition* has been installed. To enable this feature, select File→Preferences→Software License from the menu bar on the Main Screen. Refer to Software License in the Preferences section for details on viewing and changing the license options.

Initial TSM Setup

TSM Server

The TSM Server software must be at level 5.2 or later. Refer to the TSM documentation for instructions on checking and updating the TSM server.

SBAdmin Management Class

Before any backup may be performed to TSM, you must define a new management class on the TSM server called SBADMIN. All SBAdmin backups will be stored under this management class. The management class must be defined to disallow versioning of backup objects. The management class must be created using the *TSM Integrated Solutions Console* or using the following command within ***dsmadmc***:

```
DEFINE MGMTCLASS domain_name policy_set SBADMIN
```

Next, you must turn off file versioning in the ***BACKUP*** **copygroup** of the management class. This is done by setting the number of versions of each file to be kept to “1” and days to retain inactive versions to “0”:

```
DEFINE COPYGROUP domain_name policy_set SBADMIN TYPE=BACKUP \
  DESTINATION=backup_pool VEREXISTS=1 RETonly=0
```

Once the **copygroup** and management class are defined we need to activate the **policyset** with the command:

```
ACTIVATE POLICYSET domain_name policy_set
```

TSM API Client

The *TSM API Client* software is normally installed on each node when the *TSM Backup/Archive Client* software is installed. This is required by SBAdmin. To check if the API client is installed:

On AIX: Ensure the *tivoli.tsm.client.api.32bit* fileset is installed at level 5.2 or later:

```
lslpp –l tivoli.tsm.client.api.32bit
```

On Linux: Ensure the *TIVsm-API* package is installed at level 5.2 or later:

```
rpm –qa | grep TIV
```

On **Solaris**: Ensure the *TIVsmCapi* package is installed at level 5.2 or later:

```
pkginfo –l TIVsmCapi
```

2. Introduction

System Backup Administrator (SBAdmin) is designed to simplify the administration of backups on the local system as well as client backups in a networked environment. *TSM Edition* provides the ability to perform a **Full System Backup** of an AIX, Linux or Solaris *TSM client* to any *TSM server*. It does so by combining powerful backup tools with an easy-to-use graphical and web-based interface for administering backups of an unlimited number of client systems (nodes) from a central system (TSM *Admin system*). **Full System Backups** created by the *System Backup Administrator* may be used to reinstall the source system or another system with an entirely different disk configuration. Backups may be automated through the use of a backup scheduler and queuing system, and client systems may be booted from another client (configured as a *network boot server*) and installed from backups read directly from the TSM server.

In order to accommodate backups of the TSM server itself to alternate media, you may backup one TSM server to another TSM server or you may perform backups to **local tape** on each client (a configured SBTAPE device). This applies to both the TSM server and any TSM clients (in case the TSM server is unavailable).

This document will provide a description of all of the functions of the *SBAdmin – TSM Edition*, and will include instructions for performing common tasks. For additional detailed information on each option within the application, you may get on-screen help by simply clicking the right mouse button over the object in question.

This document is intended only to provide instructions on the use of the SBAdmin graphical user interface. Most tasks may be performed using the Web-based Interface, which is documented in the ***Storix System Backup Administrator Web Interface Install Guide***.

The remainder of this document provides instructions on the use of the *System Backup Administrator* (SBAdmin) graphical user interface.

Most instructions shown here may also be performed using the web-based interface and any compatible web browser. The concepts are the same, but exact instructions differ from when using the GUI interface. When using the web-based interface, refer to the *SBAdmin Web Interface Install Guide*.

The *SBAdmin Commands Reference Guide* is also available for information on running commands at the command line, some of which may be used to perform backups, verifies and restores from clients without using the administrator interface. It also describes a number of commands which may be used to perform backup administrator-related functions.

SBAdmin Terminology

It is important to understand the relationship between the different systems that will interact with the Backup Administrator software:

- **Admin System** - This is the system running the *TSM Edition* software. All clients (nodes) and backup options are configured and managed from the admin system, and the admin system will centrally perform all tasks for the clients, including scheduling and running the backup jobs, monitoring backups, performing verifies and restores, and even recreating volume groups and filesystems.

- **Server** - This is the *TSM Server* on which the backup media is attached and backups are stored. SBAdmin does not manage the TSM server, so the TSM server may be any type of system. Although there are some considerations on the TSM server, noted in the TSM Server section, the TSM server simply acts as a backup device for all SBAdmin backups, and is not managed by the *Admin System*. Select this link for more information on configuring the servers used by this application.

- **Client** - This is the TSM client (node) system from which backups will be made. The admin system must also be configured as a client (node). Select this link for detailed information on adding or

removing a client.

The clients and servers, as well as the client node information may be displayed on the main screen of the application. The application will constantly monitor the status of the clients and servers, and the icons on the screen will represent whether or not the system or device is available.

Additional terms are commonly used in this document and in the application:

- **Backup Profiles** - Any number of backup profiles may be created, which will contain the backup defaults to be used when performing a backup job. This prevents the need to answer the same questions repeatedly when configuring backup jobs. Select this link for detailed information on adding or removing a backup profile.

- **Backup Jobs** - A backup job will contain all the information needed to perform a backup, including the client(s) to backup and the server to backup to. A backup profile will be assigned to the job, which will provide most of the common backup defaults. The information in the profile, however, may be customized for each job. A backup job is identified by a Job ID and may be scheduled to run only upon demand, only once at a specific date and time, or scheduled to run on a regular basis. A backup job may contain one or more clients. If multiple clients are included in a single job, the data for all clients is referenced by the same *backup ID*. Select this link for additional information on creating, scheduling and running backup jobs.

- **Job Queues** - The SBAdmin application provides a queuing system that manages multiple backup jobs, and can prevent too many backups from writing to the same server at the same time. A queue is defined for each server for which a backup job is scheduled. Backup jobs are added to the queues when they are run. The queues may be displayed in the main screen of the application, providing an easy glance at the queue contents and the status of queued jobs, and action buttons for manipulating the queued jobs. The jobs may be started, stopped, removed from the queue or placed on hold. Running jobs may be monitored, displaying the backup progress and/or the backup output messages. Select this link for more detailed information on backup queues and how to manipulate backup jobs in the queue.

The SBAdmin System Backup

This backup contains the operating system and optionally all user data. User data may be only files in mounted filesystems, or may also contain raw data found in logical volumes (**AIX/Linux**), partitions (**Linux**) or meta-disks (***Linux/Solaris***), disk slices or ZFS volumes (**Solaris**). It is possible to reinstall the entire system from a System Backup, or even use the backup of one client to install another. Select files, directories, logical volumes and volumes groups, and even raw data may be restored from a System Backup. For information the system installation process, refer to the ***SBAdmin System Recovery Guide***.

AIX: The system backup contains the *rootvg* volume group, and may optionally contain some or all of the other volume groups on the system. If the backup is performed to **tape**, then this tape is also configured to boot to the **System Installation process**.

SBAdmin and TSM Integration

While *SBAdmin Network and Workstation Editions* provide various levels of backups to local and remote media (tape and disk), the *SBAdmin TSM Edition* focuses on what TSM customers need most - a full-system backup which can be used for complete system recovery, cloning and hardware migration. This backup can be written directly to, and restored directly from, a *TSM server*. And SBAdmin manages the TSM backups, including the backup retention and deletion. In addition, client backups can be written to **local tape** on each client. This provides the ability to keep a separate (non-TSM) system backup of any client, including the TSM server system.

SBAdmin utilizes the ***TSM Client API*** (application program interface), also referred to as an ***application client*** within some TSM documentation. Backups performed within TSM use the ***TSM Backup/Archive client***. These backups differ from those performed with SBAdmin using the API client. Backups performed by TSM are not visible within SBAdmin, and SBAdmin backups to the TSM server are not viewable within TSM. However, the same policies which apply to other TSM *management classes* and *storage pools* may also apply to SBAdmin backups.

TSM Backup Retention

SBAdmin writes backups to the "***SBADMIN" Management Class***, which must be defined on the *TSM server*. Having a separate management class for SBAdmin backups ensures that certain required policies are enforced, and allows you to assign a separate storage pool to SBAdmin backups than those used for other TSM backups.

While other TSM backups place each separate file in a backup image, and provide version control for each individual file, SBAdmin backups use a single image for each filesystem or raw device (i.e. logical volume or partition) that is backed up. SBAdmin backups, therefore, contain much less catalog space on the TSM server, and add little management workload to the server.

SBAdmin backups do not allow versioning control by the TSM server. This is because each SBAdmin backup has a unique object name. SBAdmin backup retention policies will provide the ability to control the number of backups retained on the server, as well as the age of the backups. Backups are automatically deleted from the server only when replaced by more recent backups.

Shared Versus Owner Access

SBAdmin backups to a TSM server may be designated as either *shared access* or *owner access* when the backup is created. Backups created with shared access may be restored by any other client (node). This provides the ability to create master backups which may be used for cloning, provisioning, or migration of operating systems, volume groups, filesystems, etc, to different hardware. If a backup is created with owner access, only the original node will be able to read from that backup.

TSM Server Authentication

The ***TSM Admin System*** configured for SBAdmin must be a TSM node itself (may also be the server). On the admin system, you will define the ***TSM clients*** (nodes) and the ***TSM servers***. SBAdmin does not use the TSM *client options file* (dsm.opt) nor the TSM *client system options file* (dsm.sys) defined for other applications. Instead, all clients and servers are defined on a single system (the admin system) and are copied to the clients as needed.

When a server is defined on the *admin system*, a ***TSM Administrative User*** name and password must be defined also. This TSM Administrative user must have been previously configured within TSM to have *System, Storage* or *Policy* authority. This administrative user will be used to manage the backups performed by SBAdmin. The administrative username and password is stored in a protected and encrypted file on the admin system and is never sent over the network or saved on any of the clients.

Client passwords must be defined on the admin system if the node uses ***PASSWORDAccess*** "**prompt**" to access the server. In this case, the node password will be copied from the admin system to a protected file on the client and passed to the server whenever the client accesses the server. If the node uses ***PASSWORDAccess*** "**generate**", the node password need not be defined on the admin system (assuming the node has previously accessed the server and therefore has already created a TSM encrypted password file. This is the preferred method of server authentication since it does not require the admin system to store a copy of each node's password.

Additional Notes

1. TSM exclude list processing does not affect SBAdmin backups. You must define your exclude lists (files, directories, filesystems or devices to exclude) within SBAdmin.

2. The compression option in the TSM server options will be ignored if you have set a SBAdmin backup job to use compression. To use TSM compression, turn off SBAdmin compression and turn on the compression option in the server options.

3. LAN-free backups are not supported.

4. Communication method of “shared” (shared memory) is not supported. This option would only allow a backup of the TSM server to itself, which would be useless for full system recovery of the TSM server.

5. The Tivoli environment variables used by TSM and other API client applications are not used by SBAdmin. These include *DSMI_CONFIG, DSMI_DIR* and *DSMI_LOG*. Configuration files are generated on the admin system and transferred to each client automatically. SBAdmin uses its own TSM configuration files in the ***/storix*/config/tsm** directory (where ***/storix*** is the data directory defined when you initially installed the software). This prevents any conflicts with other software using the TSM API client.

3. The SBAdmin User Interface

The SBAdmin User Interface is used for all configuration options, including servers, clients, jobs, profiles, etc. It is also used for the monitoring of job queues, displaying job status, backup output messages, and backup history.

After all backup jobs are configured and scheduled; they will continue to run even if the SBAdmin interface is *not* running. Backup jobs may also be manually started, monitored or controlled from the command line when the interface is not running, and can be monitored or controlled after the administrator is restarted.

Ordinarily, messages regarding the status of the backup jobs are reported on the screen. If, however, the SBAdmin interface is not running when a job is run, the status messages will be reported using an alternate notification method, which may be defined by the user.

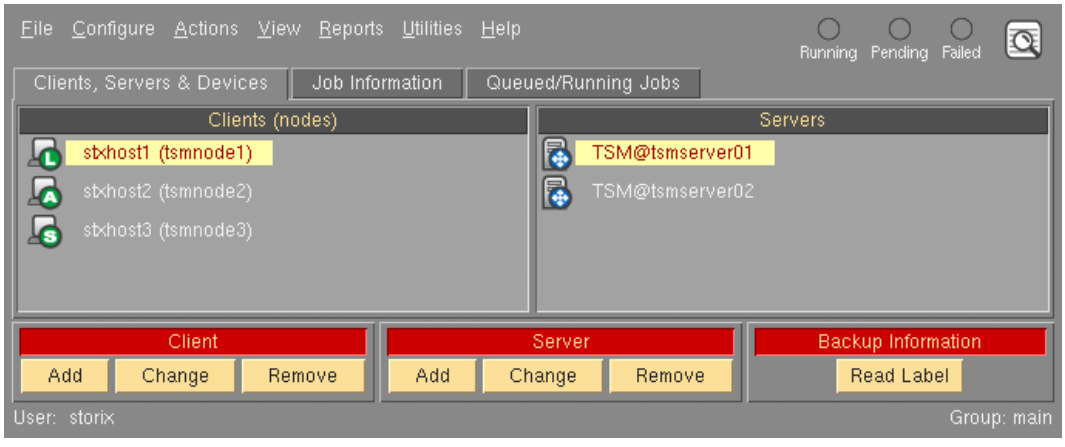
The Main Screen

The following is a sample of the **Main Screen**, which appears when the application is first started. The options at the top-left of the screen (File, Configure, etc) are contained in the menu bar. Click on any of the menu bar options to display a pull-down menu of options in each category. When selecting an option from the menu bar, a new screen, or window, will appear with additional optional options that apply to the menu selection.

At the top-right of the screen is the status bar. This contains indicators that will show green, yellow or red, indicating if there is backup job in the queue that is either running, pending (waiting) or failed, respectively. It also contains a button to view the log of backup status messages not already displayed.

The remainder of the screen will vary depending on the "Display" tab chosen:

- **The Clients & Servers** display tab is shown below. In this example, several clients and servers have already been configured. The application continually checks the availability of the systems, and displays an icon that represents both the client system type (**A**=***AIX***, **L**=***Linux, S*=*Solaris***) and whether or not the system is available (**Green**=available, **Red**=not available). Since it may not be possible to determine the Server System type, a blue server icon **(╬)** is displayed if the server is available, which will display in red if the server cannot be contacted.



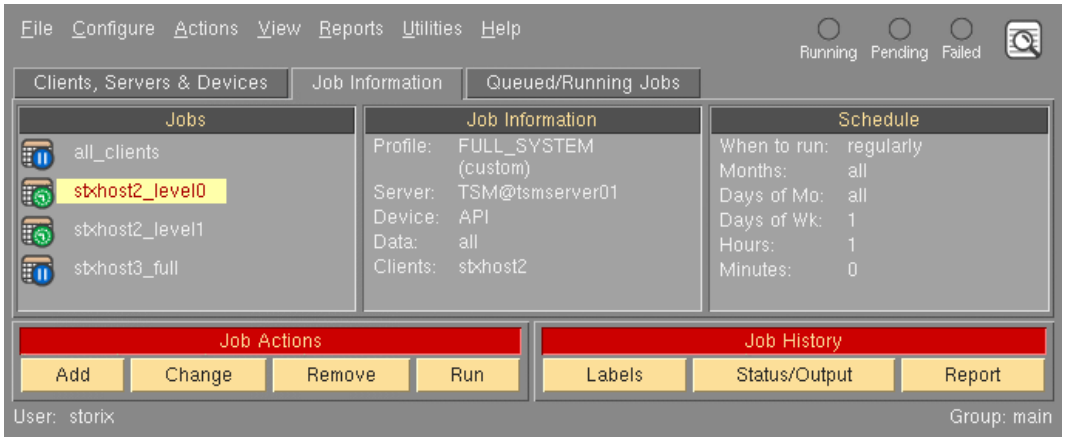
A client may be selected by clicking the left mouse button on the icon next to the client hostname. Likewise, a server may be selected by clicking the mouse button on the server icon. The *selected* client or server will appear with a highlighted background.

The action buttons at the bottom of the screen apply to the selected client and/or server. They provide a shortcut to performing the same tasks that can be performed from various options within the menu

bar. If you want to display the backup labels for all backups stored on the server, you must select a server and a client (original owner of backups to display), then press the "**Read Label**" button.

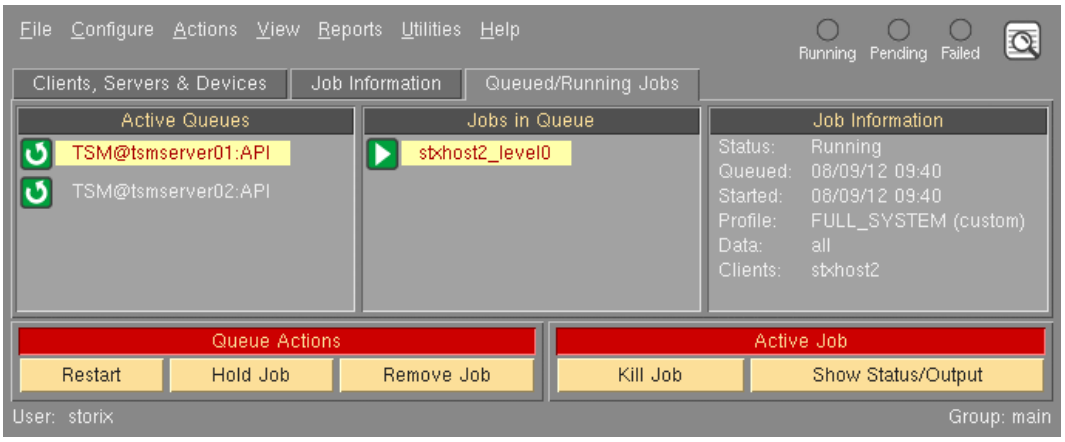
- **The Job Information** display tab provides a quick glance at the jobs that are configured. By clicking on a job icon, the job information and schedule information are displayed in the right two display areas and the job name is highlighted.

> **The**  **represents a job that is not scheduled. The**  **represents a job that is scheduled.**



The action buttons at the bottom apply to the selected job. They are shortcuts for various job-related functions. The ***Job Actions*** buttons perform the same job operations available from the Action menu on the menu bar. The Run button will place the selected job in the queue (even if it is scheduled to run at another time), and it will be run as soon as the server and device assigned to the job are available. Each of these functions is described in detail in the section Schedule or Run Backup Jobs. The ***Job History*** buttons may be used to view backup labels, status/output messages or a history report for previously run jobs.

- **The Job Queue** display tab provides a look at the jobs that are currently in the queues. A queue is shown in the left-most display area, which consists of the backup server and the device name. When you click on a queue, the selected queue is highlighted, and the jobs in the selected queue are displayed in the middle display area.



You may then click on a particular job to display the job information, including the status of the job. Both the queue and job icons represent the status of the job. The ***Queue Actions*** buttons at the bottom of the screen may be used to manipulate the selected job. The ***Active Job*** buttons include the ability to *kill* a running job or display the status or output messages of a running or failed job. All of these

functions and a list of any possible icons or status messages are described in detail in the Job Queues section.

Closing Windows

A common icon which appears at the bottom of each window is:

 **Cancel** button

After making changes to information on any screen, use the cancel button to cancel the changes and close the window. Avoid using the window-manager button (usually at the top-left of the window) to close windows as this does not always perform the entire cleanup needed. The Cancel button does not appear on the Main Screen. From the Main Screen, you should always use the File➔Exit option on the menu bar to exit the application, and you may use the icons in the title bar for other window manager functions, such as iconifying the window.

4. Users

When you first installed SBAdmin, an "**admin**" user was created and you were prompted to provide a password for this user. The admin user is given authority to all (*System Admin*) functions within the SBAdmin application, including configuring other users.

If there is only one user configured, and you are logged onto the system as "root", you are logged into the application under this user by default, and you will not need to provide a username or password at the command-line.

However, for the SBAdmin Web Interface, you must always provide a username and password.

You may configure one or more users, each with permission to perform different tasks. Each user will be assigned to a default group, but a user may be allowed access to different *groups* (see Configuring Groups).

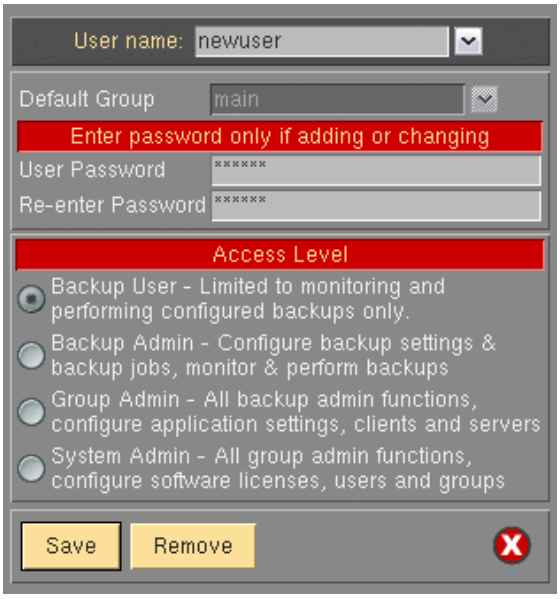
User Levels (Roles)

By configuring other users you will be able to limit their permissions and roles within the software. Configuring users at different level roles is useful if multiple people are accessing the administrator, and security policy dictates what access each person should be able to do. The following are the four types of users that may be configured within SBAdmin:

- Backup User **-** limited to monitoring backups and running backup jobs that are already configured by a privileged user.
- Backup Admin **-** allowed to configure backup settings and backup jobs. They are also able to monitor backups and run backup jobs.
- Group Admin - allowed all *Backup Admin* functions as well as configure application settings, clients and servers within their *group*.
- System Admin **-** allowed all access and may configure all backup functions as well as application settings, clients, servers and groups.

Adding a User

To add a user, select Configure→Users from the menu bar. A screen such as the following example will appear:



From this screen, type the user name in the **User name:** entry field. When adding a new user you must also specify the **Default Group, User Password**, and **Select the access level for this user** section. Press the **Save** button to add the newly configured user.

When finished, press the **Cancel** button at the bottom.

- **User name** – This field indicates the username within the SBAdmin program. This does not need to be a user defined on the Unix/Linux system.
- **Default Group** – This is the group that the user will be logged into when launching the SBAdmin interface. To allow this user to access other groups Please refer to the Groups section of this guide.
- **User Password** – These fields are for specifying or changing the user password. User passwords are encrypted and do not need to correspond with passwords on the Unix/Linux system.
- **Select the access level for this user** – This selection will determine what functions the user may perform. For more information please see the User Levels (Roles) section of this guide.

Removing a User

Click Configure→Users from the menu bar. Select the name of the user to remove from the list and press the **Remove** button. Any configurations this user may have made will remain intact; however the user may no longer log into the Administrator.

> **You must have at least one user with System Admin access to each group.**

When finished, press the **Cancel** button at the bottom.

Changing a User

Click Configure→Users from the menu bar. Select the name of the user to change from the list. Here you may enter a new password into the **User Password:** and **Re-enter Password** fields and or **Select the access level for this user**. To change the user press the **Save** button.

Users with access lower than Group Admin will only have the ability to change their password. All other fields will be disabled.

When finished, press the **Cancel** button at the bottom.

Changing your User Information

Only a user with System Admin access can add, change or remove other users. Other users can change their own information by selecting Configure→User Information or File→User Information (for users with only Backup User access).

You will see the same screen shown above, but will only be able to change your Default Group and your Password. Simply select a new default group (if more than one available), or enter a new password in the fields provided and press the **Save** button.

5. Groups

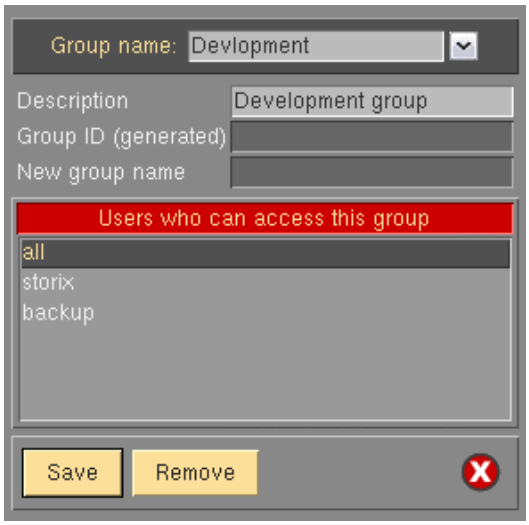
To configure Groups you must be logged into SBAdmin as a User with “System Admin” privilege.

When SBAdmin was first installed the group “main” was created. “main” will function as the default group and no further group configuration is necessary. You may choose to configure groups to assist with organization or security in your backup environment.

Groups are used to allow a single SBAdmin to organize and manage Storix Clients and Servers; and may be configured to allow or restrict certain User access. Groups are also necessary when configuring servers that will share or limit client access based on group ID. For further examples of groups please see the Using Groups section of this guide.

Adding a Group

To add a group, select Configure->Groups from the menu bar. A similar looking screen will appear:



From this screen, simply type the name of the group to add in the **Group name:** entry field and optionally a **Description** of the group. The **Group ID** field will be automatically populated with a unique value to be associated with the group. The **New group name** field is only used when changing a group. Select any users who should have access to this group from the **Users who can access this group** box. Then press the **Save** button.

When finished, press the **Cancel** button at the bottom.

- **Group name: -** This field defines the name of the group to be added.
- **Description –** This is an optional field, it is used to elaborate on and clarify what this group may be used for.
- **Group ID –** This field will be automatically populated when adding a group. It is a unique identifier and will not change if the group name is later changed.
- **New group name –** This field is only used when changing a group.
- **Users who can access this group –** This field allows you to specify one or more users that have permission to launch the SBAdmin interface under this group. For more information on users and user roles please see Configuring Users.

Changing a Group

Click Configure→Groups. Select the name of the group you wish to change from the **Group name:** drop down arrow to the right. You may now edit the **Description** and **New group name** fields or select/deselect users from the **Users who can access this group** box. Once you have made the appropriate changes press the **Save** button to update the group.

> **The "Group ID" field will never change. Once a group has been configured this value will always be used to identify the group.**

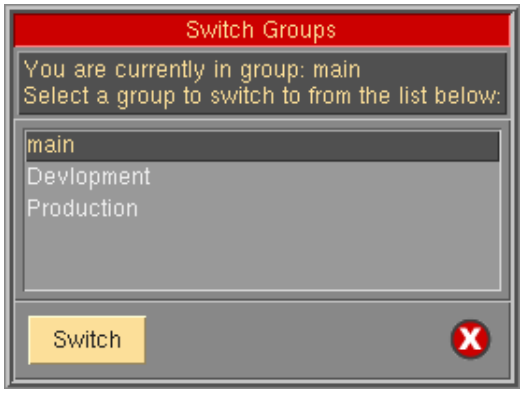
Removing a Group

Click Configure→Groups from the menu bar. Select the name of the group to remove from the list and press the **Remove** button. When finished, press the **Cancel** button at the bottom.

> **A group may only be removed after all clients and servers have been removed from the group.**

Switching Groups

Select File→Switch Group from the menu bar and Select the name of the group you would like to switch to, then press the **Switch** button. This will cause the SBAdmin interface to close and re-open under the new group. The clients, servers, media, jobs and queues will all update to reflect the settings in the new group.



> **Only one instance of the sbadmin graphical interface may run per group. You may launch multiple instances of the interface with different groups using the –G command. The following command illustrates how to launch the interface for the group "main".**
>
> **# sbadmin -G main**

6. Configuring Clients (Nodes)

A client is defined as any TSM node that will be backed up using SBAdmin.

Any number of clients may be added to the administrator as long as the total number of clients does not exceed the number of clients licensed to SBAdmin. Note that the administrator itself also includes a client license, so it may be configured as a client or server without using one of your additional client licenses.

Adding a Client

Any client may be added to the administrator by simply adding its hostname. However, the number of clients which may be added is dependent on the number of clients the administrator is licensed for. Also, any client hostname may be added, but the client is only accessible to the administrator after the software has been installed and configured onto the client system as well.

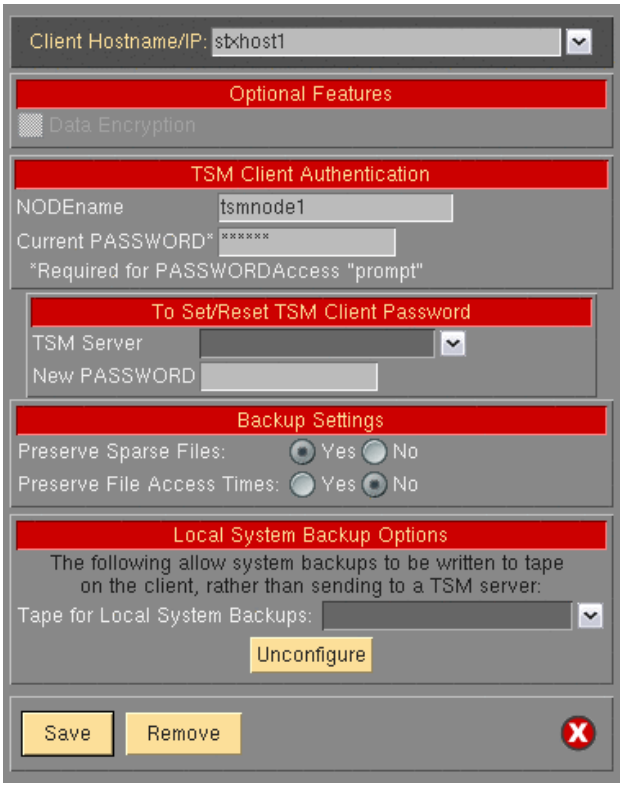
The following information is needed before configuring a TSM client:

Node Name (required)
Password (required if using PASSWORDAccess “prompt” on the server)

To add a client, select one of the following form the menu bar:

- Configure→Clients
- Click the Add Client button at the bottom of the Main Screen when the Clients & Servers are displayed.

After selecting the appropriate option above, the following window will be displayed:



To add a new client, enter the hostname of the client in the entry field at the top. Note that the hostname you enter may be a simple hostname (i.e. *ariel*), a full domain name (*goofy.storix.com*) or IP Address and must be known to the admin system. Then select any optional features that apply to this client. When you've made your selections, select **Save** to save.

To change an existing client, you may type the client name, or use the arrow button to the left of the field to select from a list of configured clients. You may then select or deselect optional features, change other entries, change the TSM password of the client on the server, or remove the client.

TSM Node Name and Password

You must enter the nodename of the client in the **NODEname** field. This is the name of the client system as known to the TSM server. The password of the client will be require if the ***PASSWORDAccess*** option of the TSM server is set to "***prompt***", since the password must be provided with each command executed between the client and server. This password will be stored on the client in a protected file, and in non-textual form, for use by SBAdmin commands.

Set or Reset the Node's Password

This screen can also be used to set or reset the password of the node on the server by selecting the **TSM Server** in the drop-down list, and entering a new password in the **New PASSWORD** field. In this case, you must also enter the **Current PASSWORD**, regardless of the ***PASSWORDAccess*** option of the server.

Enabling Backup Data Encryption for a Client

The **Data Encryption** option will be enabled only if the ***Backup Data Encryption Feature*** is installed. If so, you may select this button to indicate that data may be encrypted when backing up this client. Any type of data, for any client type, may be encrypted using 128, 192, or 256-bit AES encryption. Encryption is configured for specific clients according to the number of clients your encryption license supports. You may only select this button for the number of clients your encryption license supports.

Enabling data encryption for a client does not cause all backups to be encrypted automatically. It only designates which clients will support encryption. For clients that support encryption, the encryption option becomes available when configuring backup jobs.

To encrypt data for a client, each client must have at least one configured Encryption Key. The encryption key must be a 32, 48 or 64-byte hexadecimal number, depending on the number of bits of encryption used. An encryption key will be given a user-defined Encryption Key ID, and you may have as many Key IDs as you like. You will later select which Key ID to use when performing a particular backup.

To prevent encryption keys from ever being transmitted across the network, the encryption keys may not be configured from within the GUI interface, and client keys may not be configured from the *admin system*. Instead, you must run the **stkeys** command on each client for which encryption is to be used. Refer to **stkeys** in the ***Commands Reference Guide***, and the Encrypt data field in the backup job configuration for additional information.

Tape for Local System Backups

A client may perform a System Backup to its own direct-attached tape drive, if available. This allows any client with a tape drive to backup to itself without the use of a server or any network traffic. This tape may then be used to reinstall this client. You can move the tape or tape drive to a server to make the backup available to any client, or you can move the tape or tape drive to any other client to allow then to perform a local system recovery.

Since the tape drive names may differ for each client, you will select in this field the name of the tape drive to configure. Only tape drives that are configured and available on the client will be shown. Although multiple tape drives may exist, you may only select one drive per client for system backups.

Note that this option will create a special tape device with the name "**SBTAPE**". This device will then be available when you configure a backup job and indicate the backup is to a local tape device. Refer to Creating a Local System Backup in the job configuration for more details.

Sparse File Handling

A sparse file is a file in which blocks of data have been written non-sequentially, leaving unallocated blocks in the middle of a file. If the sparseness of a file is not preserved when restoring, the file will be expanded to include all blocks in the middle of the file, often causing a filesystem to inadvertently run out of space.

Preserving sparseness in files is usually desirable. This is sometimes a problem, however, if your files were pre-allocated using ***NULL*** characters. If a file is created and all blocks are allocated by writing nulls, or "0"s, throughout the file, the file appears identical to a sparse file on the backup. Since files containing null blocks are indistinguishable from sparse files, the blocks are not retained upon restore. The affect is that a file created at a large size could be restored to a very small size.

To resolves this issue, you may select the **Preserve Sparse Files** option so that all backups of this client will be created without preserving the sparseness of files. Therefore, if a file was pre-allocated using NULL blocks, the null blocks will also be restored. Note that, when using this option, a truly sparse file (created without pre-allocating blocks by writing nulls) will be interpreted as a large file of null blocks, and will be expanded upon restore in order to retain the null blocks. This will often cause the filesystem to run out of space since a file that was once very small is restored quite large.

If a backup is created by preserving sparseness, which is the default, then the backup files may not be restored to another system of a different operating system type. If you want to restore a backup to a different operating system type, then you should turn OFF sparse file handling BEFORE creating the backup.

Press the **Save** button to add or change the client settings. After adding a client, its icon will immediately appear on the Main Screen when Clients, Servers & Devices are displayed. If the software has not been configured on the client, or if the client was not configured using the correct hostname of the admin system, the client icon will appear in red. If the software is installed and configured properly on the client, the icon will appear green to indicate that the client is accessible to the admin system.

Removing a Client

A client may be removed from the system only if it is not assigned to any backup jobs. If it is, you will be informed so, and you must remove or change the job to remove the client from the list of clients to backup.

To remove a client, either:

- Select a client on the Main Screen when Clients & Servers are displayed, then click the **Remove Client** button at the bottom of the screen, or
- Click Configure→Clients from the menu bar. Select the name of the client to remove and press the **Remove** button.

The client icon will be removed from the Main Screen when Clients & Servers are displayed.

7. Configuring TSM Servers

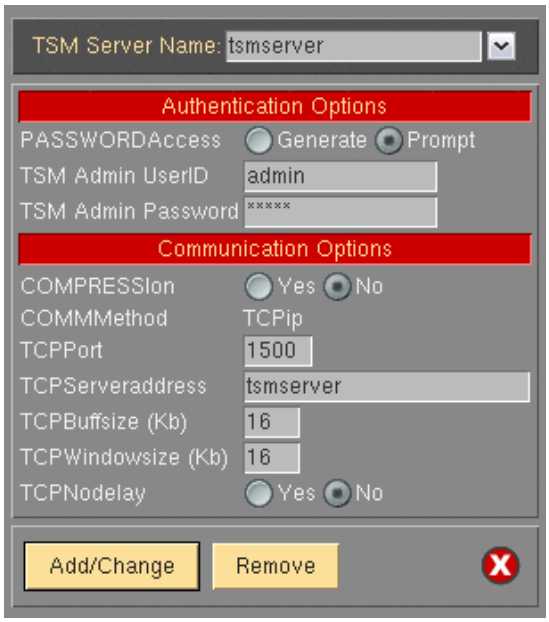
Any TSM server, and any number of TSM servers may be configured for use by SBAdmin TSM Edition. This is not limited by the number of client licenses installed. In addition, a single physical TSM server may be accessed using different TSM server configurations. For example, one server (*tsmserver-comp*) may be configured to backup data using TSM compression, while the same server (*tsmserver-nocomp*) may be configured to backup without using data compression.

Adding a TSM Server

A new server may be added to the system by either:

1. Selecting Configure→Servers from the menu bar, or
2. Pressing the **Add Server** button at the bottom of the Main Screen when Clients & Servers are displayed.

After doing so, a screen similar to the following will be displayed:



You should refer to your TSM documentation for information on the additional fields which are normally specified in your TSM system user options (***dsm.sys***) file. You may use the right-arrow button over any field to show the *QuickHelp* information on each field, so information is not detailed here. However, there are some special considerations:

TSM Server Name

You can call the server anything you like, since it is the entry in the *TCPServeraddress* field, not the server name, which determines how the server will be contacted. You can also configure multiple servers, each with a different name, that use the same *TCPServeraddress* entry.

TSM Admin User ID/Password

You must enter the name and password of a TSM administrative user already configured on the *TSM server*. This administrative must have been configured with either ***System or Policy authority***. The administrative user ID entered will be used only by this SBAdmin application to perform management tasks on behalf of the clients. This information is never sent to or saved on the TSM client systems.

PASSWORDAccess

If this field is set to "**generate**", it is assumed that you have already set the password on the client using another TSM application (or have run another type of TSM backup from this client), and the server used had this option set to "generate". In doing so, an encrypted password file was created on the *TSM client*, and will be used by this application also. In this case, you do not need to enter a **Current PASSWORD** when configuring the TSM clients.

If this field is set to "**prompt**", the client password must be provided each time contact is made with the TSM server. The password is stored on this TSM *Admin system* for future use, and is also sent to the client and stored in an encrypted and protected file for use by SBAdmin commands. Normally, the password is contained in the client user options file (***dsm.opt***). However, SBAdmin does not use this file but supplies the password to the TSM server with each command. When using this option, you will need to enter a **Current PASSWORD** for each TSM client you configure.

COMMMethod

This will be displayed as "TCPIP", which is the only option supported. The only other TSM option is "shared" (shared memory), which can only be used when backing up the server itself. The shared memory option provides no significant performance increase and is not supported by SBAdmin.

COMPRESSion

A selection of "yes" simply indicates that TSM will compress backup data on the client before sending to the server. SBAdmin provides its own compression options (see Configuring a Backup Profile). If you choose to use SBAdmin compression, then no TSM compression will be used *regardless of your selection here*. If you want to use TSM compression, you should select "yes" in this field, and do *not* indicate to use compression within your backup profile (default). Different compression schemes work best on different types of data and sizes of files. You should experiment with using both TSM and SBAdmin compression options to determine which provides the best compression with the least impact on the client system performance.

To add a new server, enter a name in the entry field at the top, add or change any of the fields on the screen, then click the **Save** button.

Changing a Server

The information for an existing server may be changed by either:

1. Selecting Configure→Servers from the menu bar, or

2. Selecting a server icon from the Main Screen when the Clients & Servers are displayed, and pressing the **Change Server** button at the bottom of the screen.

If selected from the main screen, the server options screen will appear with the prior settings for the server. If not, select the server by typing the name at the top, or use the arrow button to the left of the entry field to select from a list of configured servers. Simply add or change any of the information on the screen, then press the **Save** button at the bottom to save the changes.

Removing a Server

Removing a server, in this case, removes the configuration from the SBAdmin interface, but has no affect on the TSM server itself. A server may be removed only if there are no jobs currently assigned to it. If there are jobs assigned, you will be informed so, and you must remove or change the job to use a different server before the server may be removed.

To remove a server, either:

Select Configure→Servers from the menu bar, then select the server by typing the name at the top, or use the arrow button to the left of the entry field to select from a list of configured servers. Then press the **Remove** button at the bottom of the screen.

Select a server icon from the Main Screen when the Clients & Servers are displayed, then press the **Remove Server** button at the bottom of the main screen.

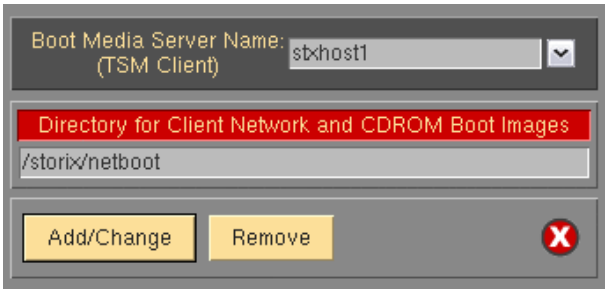
8. Configuring Boot Media Servers

A boot media server is a system used to store client CDROM ISO and network boot images created by SBAdmin. When creating boot media, you will be given the option to store the images on a boot media server. When the images are successfully created, they will be copied to the specified directory on the boot media server. You will then burn the ISO to a CD/DVD and use the disc to boot a client into the system recovery process. If utilizing network boot images, then the images will be used to perform a network boot of the client into the system recovery process. Boot media is described in detail in the ***SBAdmin System Recovery Guide***.

> **You may have multiple boot media servers. However, only a configured TSM client may be configured as a boot media server.**

Adding a Boot Media Server

A new backup media server may be added by selecting Configure→Servers→Boot Media Servers from the menu bar. The following window will appear:



To add a boot media server, enter the **IP address or hostname** of the boot media server in the entry field at the top of the window. Note, that the boot media server must already be configured as a TSM client within SBAdmin. Specify the directory on the boot media server you wish to store the images in the **Directory for Client Network and CDROM Boot Images** field and press the **Add/Change** button to save the configuration.

Changing a Boot Media Server

You may view or change the current configuration of a boot media server by selecting Configure→Servers→Boot Media Servers from the menu bar. Enter the boot media server name in the entry box at the top of the window, or select the arrow button to the right of the entry field and select an existing server from the list.

The settings for the server will then be displayed. If you wish to make a change to the server configuration, simply add or change any of the information on the screen, then press the **Add/Change** button at the bottom to save the changes.

Removing a Boot Media Server

You may remove a boot media server by selecting Configure→Servers→Boot Media Servers from the menu bar. Enter the boot media server name in the entry box at the top of the window, or select the arrow button to the right of the entry field and select an existing server from the list.

The settings for the server will be displayed. If you wish to remove the server, then press the **Remove** button at the bottom of the screen. Removing a boot media server will have no effect on its client configuration but you will no longer be able to perform a network boot using this server.

9. Backup Profile

A backup profile is used to set default backup selections commonly used when performing backups. Assigning a backup profile to a backup job alleviates the need to repeatedly answer the same questions every time a new job is added.

> **At least one profile must be created. When the software is first installed, a pre-defined FULL_SYSTEM backup profile is automatically installed. This profiles is not required if you create others, and may be removed if desired.**

After creating a single backup profile, any options selected for that profile may be customized for each backup job it is assigned to. You may want to create different profiles to prevent having to change the options for different jobs.

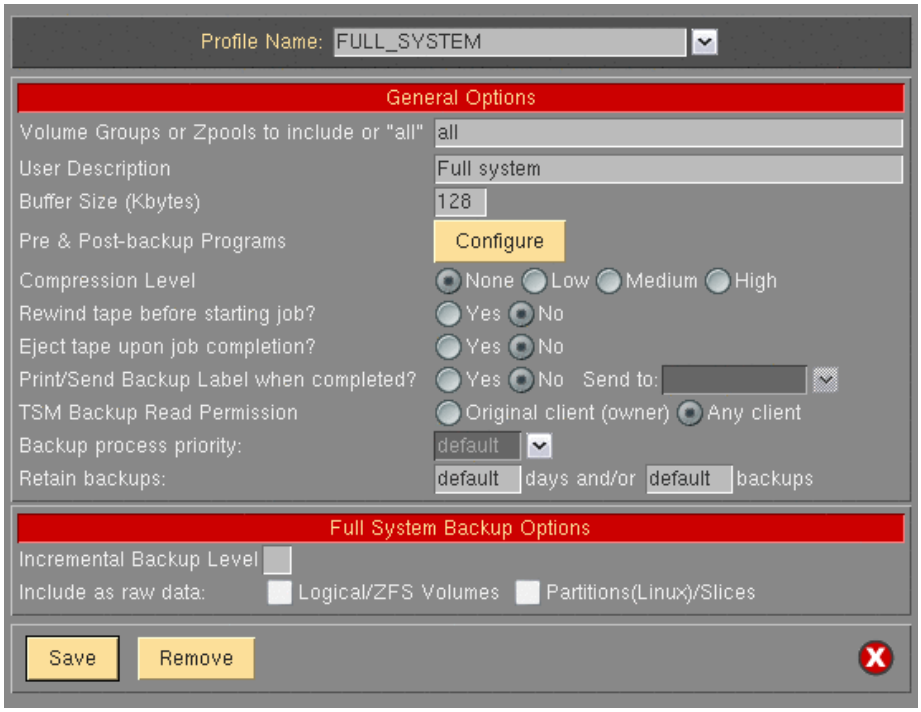
Adding a Backup Profile

A new profile may be added by selecting Configure→Backup Profiles from the menu bar.

There is one pre-defined profile configured when the software is installed. You may choose to edit this profile, delete it, or add new ones of your own.

> **The options may vary depending on the operating system support and additional features enabled. Refer to Operating Systems Support and Enabling Optional Features for more information.**

The following is an example of a **System Backup** profile when ***Linux, Solaris*** and ***AIX*** client support is enabled:



To add a new profile, enter a new **Profile Name** in the entry field at the top of the screen. A profile name may consist of any characters except a colon (:) or space (spaces will be changed to underscores).

Note that after assigning a profile to a backup job, you may customize the profile further for the specific job. Therefore, it is required that only one backup profile exists. Refer to Configure a Backup Job for more information.

Use QuickHelp at any time to display a description or instructions for a particular option. Most options are described in detail in the help information and are therefore not shown here. There are a few special considerations:

Buffer Size

The buffer size represents the amount of data to accumulate in memory before writing that "buffer" to the backup device. In actuality, SBAdmin uses many buffers for best performance, but the amount of data written to any device at one time is set using the **Buffer Size** option.

Using a buffer size larger than the physical device can handle will result in an I/O error writing to the device, which generally varies by operating system or device driver. The default of 128K is adequate for most devices without exceeding their hardware limit. However, for best performance, especially when using high-speed tape drives, disk drives and RAID devices, you can increase this number. A value of 512 or 1024 is often best.

Note that, while not excessive, a larger buffer size will cause SBAdmin to use more memory during a backup. Also, if you use a large buffer size, you may see a backup slow down if the system is unable to write a large buffer to the device fast enough, or if there is limited memory on the system. For this reason, it's best to experiment with different buffer sizes until you find the best backup performance for your device.

Specifying the Data to Backup

The description of the first field in the **General Options** section will differ based on the backup type you selected for this profile. In this field, you may enter the ***data to backup***. This information is not required at this time and may be filled in when configuring the backup job later. Because TSM Edition only supports "*full system"* backup types, the type of data in this field will be either volume groups (Linux/AIX) or ZFS pools (Solaris). You may also enter "**all**" to include all volume groups or ZFS pools. You may also enter a list of options to *exclude*. For example, to include all volume groups EXCEPT the "tempvg" volume group, type:

```
all –tempvg
```

If you want to exclude all volume groups and ZFS pools you may leave this option blank. Leaving this option blank does have different effect depending on the type of client the backup is performed on. On an ***AIX*** system, leaving this option blank will still include the **rootvg** volume group (required on a base system). It will also include all volume group definitions of currently defined volume groups but will not backup the data within the excluded volume groups. On a ***Linux*** system, leaving this option blank will exclude all LVM data including their definitions and data. Likewise, leaving the field empty on a ***Solaris*** system will exclude all filesystems and volumes contained in *ZFS pools*.

If any items within the data list do not apply to a client, the item will simply be ignored. For example, using a data list containing the volume group "VolGroup00", a client without a VolGroup00 volume group will simply skip this volume group.

Compression Level

As noted in the Configure Servers section, there are two methods of compression which may be applied to backup data – TSM and *SBAdmin compression*. By default, no SBAdmin compression will be used (this field will be set to "***None***").

A selection of "yes" simply indicates that TSM will compress backup data on the client before sending to the server. It is important to not, however, that SBAdmin provides its own compression options (see Configuring a Backup Profile). If you choose to use SBAdmin compression, then no TSM compression will be used *regardless of your selection here*. If you want to use TSM compression, you should select "yes" in

this field, and do *not* indicate to use compression within your backup profile (default). Different compression schemes work best on different types of data and sizes of files. You should therefore experiment with using both TSM and SBAdmin compression options to determine which provides the best compression with the least impact on the client system performance.

TSM Backup Read Permission

It is important to note the **TSM Backup Read Permission** field in the backup profile because this will determine if the backup of this client (node) will be readable by another client (node). When a backup is created, it is stored in a *TSM filespace* that corresponds to whether the backup should be private (owner-access only) or shared (any node can access).

If node data should not be accessible between nodes, be sure to set this option to "***Same client only***". Otherwise, select "***Any client***".

Note that if you have created a backup that you wish to have installed onto different nodes, such as system replication (cloning), you must make that a shared backup. Otherwise, only the original node can access it.

Incremental Backup Level

Using this field, you may create *incremental* (or *differential*) backups of the system. An incremental backup must be based on a level 0 (full) backup. Therefore, you must always perform a level 0 before any subsequent levels.

If you do not plan to perform incremental backups, it's best to leave this field blank to avoid unnecessary time processing incremental information for the backup.

If you set this field to "0", then a full system backup will be performed, from which you may base additional incremental backups. Any number (1-9) indicates that you will be performing a new incremental backup, which will be based on the previous backup level.

Note that you will not be able to perform any incremental backups (levels 1-9) until you have performed at least one level 0 backup.

A Level 0 incremental (or a system backup *without* an incremental level) is the only backup from which the system may be re-installed.

A system backup with no *incremental* level specification, or a system backup with incremental level 0, is required to re-install a system. Only after the system is restored from this full system backup can you restore additional incremental backup levels. Refer to Incremental/Differential Backups for more general information and examples.

Backup Retention Policy

By default, all backups will be retained or overwritten according to Backup Retention Policy set in the Preferences section. However, certain backups or types of backups you may wish to retain for a longer period of time. For example, you may want to retain a full backup taken at year-end for several years, while a daily backup (replaced on a daily basis) may only need to be retained for a week. Rather than choosing to retain a backup for a certain number of days, you can also choose to retain a certain number of backups of the same job.

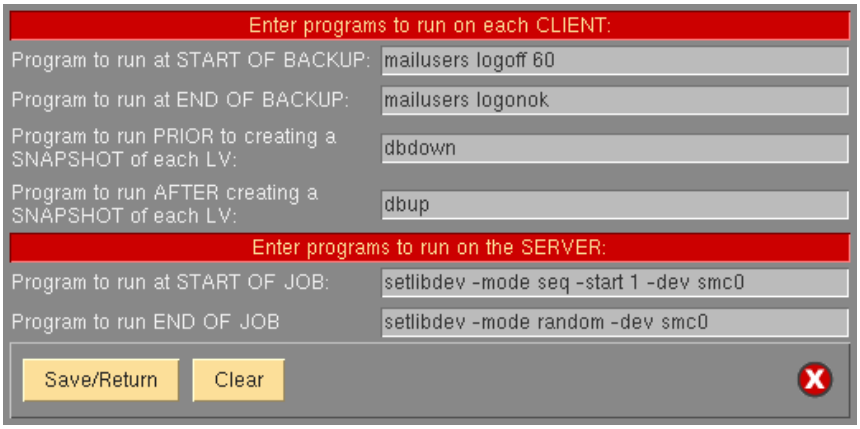
If you set a retention policy in the profile settings, it will override the policy set forth in the ***Preferences***. If you choose to customize a profile for a specific job, it will apply only to backups created by that job and will override the policy for both the main profile and in the ***Preferences*** section.

For details on the use of the **Retain backups** field, refer to Backup Retention Policy set in the Preferences section.

After making all selections, save the profile by pressing the **Save** button at the bottom. The information will be saved and the window will be closed.

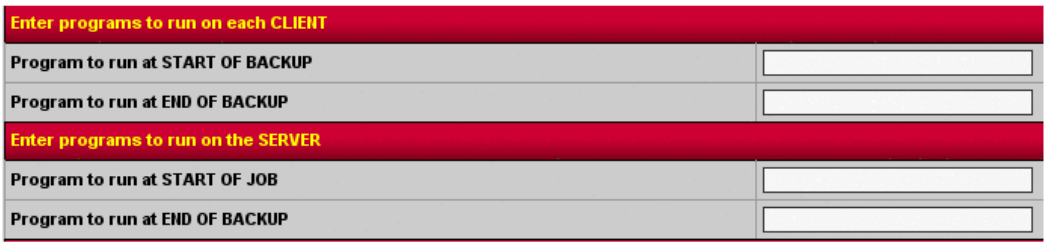
Pre-backup and Post-backup Programs

Within the backup profile, you may configure a program to run on the client, before and/or after the backup command runs. You can also select to have programs execute before and after the creation of snapshots used for backups. This program, either a *pre-backup* program or *post-backup* program, is a custom program which exists on one or more clients, and may perform any operation, such as starting and stopping database programs, forcing users to log off the system, etc. To configure pre- or post-backup programs, press the **Configure** button next to the ***Pre & Post Backup Programs*** field. When doing so, the following screen will appear:



Note that the options for running programs prior to or after creation of snapshots are only available with backups of data contained in JFS2 filesystems (AIX), LVM logical volumes (Linux) and ZFS filesystems (Solaris).

Using the web interface is slightly different. You will notice the option to configure pre and post backup programs directly from the main profile configuration screen:



The pre-backup and post-backup programs will be executed with **ROOT USER** authority. Therefore, they must be placed in the ***DATADIR*/custom** directory by the root user on the client (where *DATADIR* is the directory you selected on each system when SBAdmin was configured - i.e. */storix*). The *custom* directory is owned by the root user and only the root user on each system has the ability to add files to this directory. The commands placed in the custom directory may be shell scripts or binary programs and must have *execute* permission.

To configure a pre-backup or post-backup program, simply add the name of the program to the profile in either of the **Pre-backup Program** or **Post-backup Program** fields. Do not enter the full path name of the program, only the file name. The program is assumed to be in the ***DATADIR*/custom** directory. You may also add optional arguments to the command, separated by spaces.

Pre & Post Backup Programs

When a backup job using a profile containing client pre-backup or post-backup programs is run, the system will attempt to execute the specified program on each client before or after that client backup is performed. If the program does not exist on any client or is not executable, it will be ignored. Otherwise, it will be executed and one of the following actions will be taken depending on the exit code of the program:

	Pre-backup Program	Post-backup Program
Exit code 0	Client will be backed up and the job will continue normally.	Job will continue normally.
Exit code 1	Client will not be backed up and the backup job will be terminated with an error message	Job will terminate with an error.
Exit code 2	Client will not be backed up. If there are other clients to backup, the job will continue normally. However the job will complete with warning messages.	Job will continue normally. However, the job will complete with warning messages.
Exit code 3 or higher	Client will be backed up and the job will continue normally. However, the job will complete with warning messages.	Job will continue normally. However, the job will complete with warning messages.

A post-backup program will be executed even if the backup command that precedes it fails. This is necessary in case the post-backup program must record information about the backup or restart processes that were stopped by the pre-backup program.

Pre & Post Snapshot Programs

When a backup job using a profile containing pre-snapshot and post-snapshot programs is run, the system will attempt to execute the specified program on each client before and/or after each snapshot is created.

The program will only be executed for the storage containers to be included in the backup, and if Snapshot Backups have been configured and the Backup Job is configured to perform snapshot backups.

The program names provided will be executed before a snapshot is created for *each logical volume/filesystem*. Therefore, the program must be intelligent enough to recognize the name of the logical volume or filesystem the snapshot is being created for at that time and act accordingly (or do nothing). Refer to Creating Pre and Post Backup Programs below for more information.

If the specified program does not exist on any client or is not executable, it will be ignored. Otherwise, it will be executed and one of the following actions will be taken depending on the exit code of the program:

	Pre-snapshot Program	Post-snapshot Program
Exit code 0	The snapshot of the logical volume will be created and the backup will continue.	Backup will continue normally.
Exit code 1	The snapshot will not be created for the logical volume and the backup will terminate.	The backup will terminate with an error.
Exit code 2	The snapshot will not be created for the logical volume, and the backup will continue using the active (online) data.	The backup will terminate with an error.
Exit code 3 or higher	A warning message will appear, but the snapshot will be created and the backup will continue normally.	The backup will terminate with an error.

Creating Pre & Post Backup Programs

A customized program may perform any function on the system since it is run under *root user* authority. Any arguments or flags may be provided to the command. The same script may be called with arguments that tell the script how to proceed. For example:

`mypreprogram –kill`	may be used to log off users and
`mypreprogram –warn`	may warn users of the backup only, or
`mypreprogram –kill 60`	may warn users, then log them off after 20 seconds, etc.

In many cases, it is desirable for the program to have certain information about the backup job. The program may want to display or save information about the backup job in another application or file, or a post-backup program may need to respond differently depending on whether the backup was successful or not. Every program will have access to the following environment variables:

STX_CLIENT	The name of the client
STX_SERVER	The name of the TSM server
STX_DEVICE	The name of the device on the server (API if written to TSM server)
STX_JOBID	The Job ID
STX_BACKUPID	The Backup ID
STX_EXITCODE	The exit code of the backup command or job
STX_SNAPLVNAME	The logical volume/filesytem for which a snapshot is created.
STX_SNAPFSNAME	The filesystem name (mount point) of the snapshot This will show a dash "-" if the snapshot is not a filesystem

The **STX_EXITCODE** variable is only used in client post-backup/job programs. This indicates the success or failure of the backup.

The software is installed with sample script programs that may be used for any client or server pre-backup, post-backup or pre/post snapshot program. The programs are called “**prepost.sample**” and "**prepostsnap.sample**" and will simply display the values of all of the above variables when the backup job is run. You may edit or view the contents of this script file (contained in the ***DATADIR*/custom** directory), which contains additional details on the use of this option.

Incremental/Differential Backups

An *incremental backup* is on in which the only data to be included in the backup is that which has changed since the prior incremental backup level. An incremental backup level can be from 0 to 9, where 0 is a “full incremental” backup from which all other levels are based. Levels 1 through 9 indicate that only data that has changed since the last ***prior-level*** backup should be included.

Differential backups are also incremental backups, except that backups include a cumulative list of files that have changed since a certain time. This is achieved by running the same incremental level backup repeatedly, backing up the same files that changed since the last prior-level (or level 0) backup, along with any additional files that have changed since the last time the same incremental level backup was run. The result is that the backup gets continually larger each time it is run, until a prior level (or level 0) backup is run again.

Raw devices such as *logical volumes* (***AIX***) and other partitions (slices or *ZFS volumes* on ***Solaris***, meta-disks on ***Solaris*** & ***Linux***, etc) that do NOT contain mounted filesystems will always be backed up in their entirety if they have been written to since the last backup of a prior level. This assumes that you selected to “**Include as raw data**” this information in the backup profile. If included, we assume in the examples below these raw devices will be included with the backups as well as the “files”.

Incremental Backup Examples

1. Consider the following backup schedule:

Monday	**Level 0**
Tuesday	**Level 1**

Wednesday	**Level 2**
Thursday	**Level 3**
Friday	**Level 4**

a. On Monday, the entire system will be backed up. Note, however, that only the volume groups indicated in the backup profile will be included, if applicable.

b. On Tuesday, only the files that have changed since Monday's backup will be included in the incremental level 1 backup.

c. On Wednesday, only files backed up since the last ***prior-level backup*** (level 1) will be included in this backup.

d. Likewise on Thursday and Friday.

e. On the following Monday, a new incremental level 0 is performed, backing up all data once again. This is the new backup from which all subsequent backups will be based. Any incremental backups performed prior to this level 0 will be considered obsolete.

2. In a second example, consider the following backup schedule, which is often referred to as ***differential*** backups since we're effectively backing up the differences between the system as it is now versus a specific day in the past :

First day of the Month	**Level 0**
Each Friday night	**Level 4**
Each other weekday	**Level 7**

a. On the first day of every month, regardless of the day of the week, a full incremental backup is performed.

b. The next day, an incremental level 4 will be performed (if Friday) or an incremental level 7 will be performed (if Monday through Thursday)

In this example, keep in mind that it is not necessary to perform a level 1 backup after a level 0, since each level (1-9) will backup the data from the last ***prior-level*** backup performed, even if it was several levels prior. Therefore, if your last level was 0 (full), then either a level 4 or a level 7 will backup the same data. However, if your last level was 4, a level 7 will always backup files changed only since the last level 4.

In addition, each weekday the *same* backup level will be performed. Since all data will be backed up since the last ***prior*** level, your previous day's backup of the same level will become obsolete.

3. This example is a ***differential*** backup, where all backups are based on the most recent level 0 (full) backup that was performed:

Every Friday night	**Level 0**
Monday through Thursday night	**Level 1**

a. Every Friday night, a full backup level 0) is performed.

b. On every other night, a level 1 backup is performed. The result is that, each day, all files that have been created or changed since the Friday night backup will be backed up again. The size of the backup will grow each day until after the next Friday night backup is again performed.

Restoring from Incremental Backups

If re-installing the system from the backup, you must always restore from a level 0 incremental backup (or one that did not use an incremental level). The system installation process will not allow you to select an

incremental level (1-9) to restore from. Only after the system has been reinstalled and rebooted will you be able to restore additional incremental levels using the SBAdmin interface.

From a full-system backup, you can restore files, directories, filesystems or specific volume groups onto a running system. If your system backup is an incremental backup and you choose to restore filesystems or volume groups, the backup will be restored as an incremental backup as described below:

There are a few things to remember when restoring from incremental backups in order to get your data back to the most recent state:

a. Always start by restoring from your most recent incremental level 0. This will remove and replace all files in each filesystem.

b. Always restore full **Volume Groups/ZFS Pools** or **Filesystems** from incremental backups. If you choose to restore a *directory* from a full-system backup, all files will be restored from the backup, but changes will not be re-applied, such as re-removing files which had been removed prior to that incremental backup level.

c. Restore incremental levels in the order they were performed ONLY if the next incremental level to restore is more recent than the last. For instance, if you performed a level 1 backup most recently, do not restore a level 2 backup which is older than your level 1.

d. When you perform the same incremental backup level multiple times without performing a lower-level, restore only the most recent backup of that level. Any prior versions of the same backup level are considered obsolete.

In the first backup example above, you must restore each backup, starting with level 0 in the order of each backup level, stopping when you encounter a backup level that is older than this predecessor. If your level 1 backup was most recent, then you will need to restore only level 0 and 1. If your level 4 was most recent, you will need to restore all levels 0 through 4.

In the second example, you are ensured never to have to restore more than three backups to get your data up-to-date. This convenience comes with some complication when restoring. First, you must of course always start by restoring your last level 0. Then, if there was a higher level backup performed after your level 0, restore it next (it could be a 4 or 7 depending on what day is the first day of the month). Lastly, if you restored a level 4 and there was a level 7 backup performed after your level 4, restore it next.

Changing a Backup Profile

The information for an existing profile may be changed by selecting Configure→Backup Profiles from the menu bar. The profile options screen will then appear. Either enter the name of the profile in the field at the top of the screen, or select the arrow button to the left of the entry field and select an existing profile from the list.

The profile settings will then be displayed. Simply add or change any of the information on the screen, then press the **Save** button at the bottom to save the changes.

Removing a Profile

A profile may be removed from the system only if it is not assigned to any backup jobs. If it is assigned to a job, you will be informed so, and you must remove or change the job to use a different backup profile before the current profile may be removed.

To remove a profile, select Configure→Backup Profiles from the menu bar, enter or select the profile to remove, then press the **Remove** button at the bottom of the screen.

10. Exclude Lists

Exclude lists are used to exclude certain files, directories, or devices (such as partitions or logical volumes) from backup jobs. You may create any number of different exclude lists, and assign *one or more* exclude lists to a particular backup job. You may also select which clients the exclude list will apply to. This allows you to use an exclude list for a job, but still have it only apply to certain clients if multiple clients are backed up by the same job.

Note that you can specify the volume groups to include or exclude (i.e. “all –appvg”) in your backup job. It is therefore not necessary to exclude a volume group or its contents using an exclude list if it was not included on the job. Using an exclude list as described in this section, however, will provide the ability to exclude specific files or directories within the filesystems.

Exclude lists may be used to exclude files, directories, entire filesystems or *device data* (such as partitions or logical volumes) from your full-system backup. *Wildcard* characters (*) in exclude list entries may also be used to exclude may files or directories matching a certain pattern.

Device names may also be added to the exclude list. A device name may be an LVM *logical volume*, *meta-disk* (software RAID) device name, or disk *partition*. The data within the device will only be excluded if it is *not* used for a filesystem. To exclude a filesystem, you must exclude the filesystem mount point (directory).

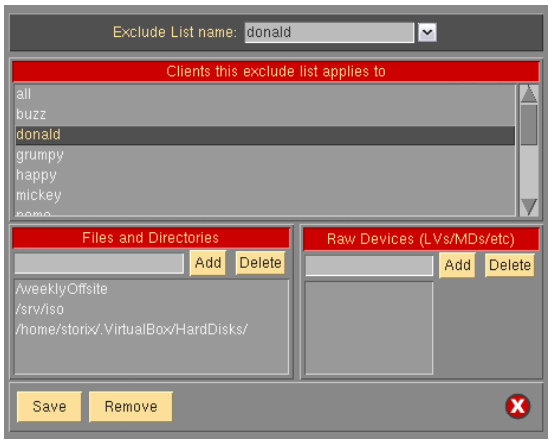
Using Wildcards

If you wish to exclude a directory, all files within the directory as well as any sub directories will also be excluded. A ***wildcard*** (*) may be used in an exclude list entry for files and directories. For instance, having **/usr/local/*.old** in the exclude list will exclude all files in the /usr/local directory with a “.old” extension. Wildcards in the exclude list work the same as at the command line. For example, typing “`ls /usr/local/*.old`” will yield the same list of files that will be excluded if */usr/local/*.old* is in the exclude list. You may specify multiple wildcards in the same string. For example, “*/*/local/x*.old*” will exclude files starting with an “x” and ending with “.old” in the /usr/(*anydir*)/local directory.

> **You may not use other special characters in exclude list entries, even if they exist in the names of the files to exclude. Those characters are $, +, ? and ^, which have special meaning to the system.**

Adding an Entry to the Exclude List

Select Configure→Exclude Lists from the menu bar to display the following **exclude list screen**:



You may enter a new **Exclude List name** in the entry field at the top of the screen, or select an existing exclude list name using the arrow button to the left of the entry field. When doing so, the current settings for the selected exclude list, if any, are displayed.

In the first (**Clients**) listbox, you may select "**all**" to apply this exclude list to all *clients* (when assigned to a backup job), or select individual clients the exclude list should apply to. Note that, if this exclude list does not apply to a particular client, that exclude list will not appear as a selectable option when configuring a backup job. If, however, the exclude list is applied to a client, this does not automatically apply to all jobs. You must also select to use the exclude list (or lists) when configuring a backup job.

To exclude files or directories, type the file or directory name (or wildcard string) in the entry field under the ***Files and Directories*** heading. To add a *logical volume, partition* (***Linux***), *slices* and *ZFS volumes* (***Solaris***) or *meta-disk* (***Linux/Solaris***) to the exclude list, enter the device name (do not prefix with /dev) in the entry field under the appropriate heading. Note that the heading will only show the device types that are supported for the various client operating system types enabled.

Press **Enter** or select the **Add** button next to the corresponding entry field to add the item to the list.

When all selections have been made, press the **Save** button at the bottom of the screen to save the entries and clear the entries. To undo all changes made, press the cancel button at the bottom.

Removing Entries from the Exclude List

To remove an entry from the exclude list, display the exclude list screen by selecting Configure→Exclude Lists from the menu bar and selecting the exclude list to change. Then, to remove a file or directory entry, select the item in the ***Files and Directories*** listbox and press the **Remove** button next to the file or directory entry field. Likewise, to remove a logical volume from the list, select the item in the ***Raw Devices*** listbox and press the **Remove** button next to the entry field. When you have removed all desired selections, press the **Save** button at the bottom of the screen to save the remaining entries and exit. To undo all changes made, press the cancel button at the bottom.

To remove an entire exclude list, select Configure→Exclude Lists from the menu bar, enter or select the exclude list at the top of the screen, then press the **Remove** button at the bottom of the screen. Note that, when removing an exclude list that is assigned to current backup jobs, the exclude list will be removed from the job configuration. You will be informed if the exclude list is assigned to any jobs before proceeding.

11. Backup Jobs

A backup job must be created before any backup may be performed by the *admin system*. The job information will identify the TSM server and one or more clients to backup and the backup profile. If the backup is to be scheduled to run either at a later time or on a regular basis, the dates and times are also added to the backup job information. Temporary backup jobs which are run only once may also be set to be automatically deleted once the job has completed.

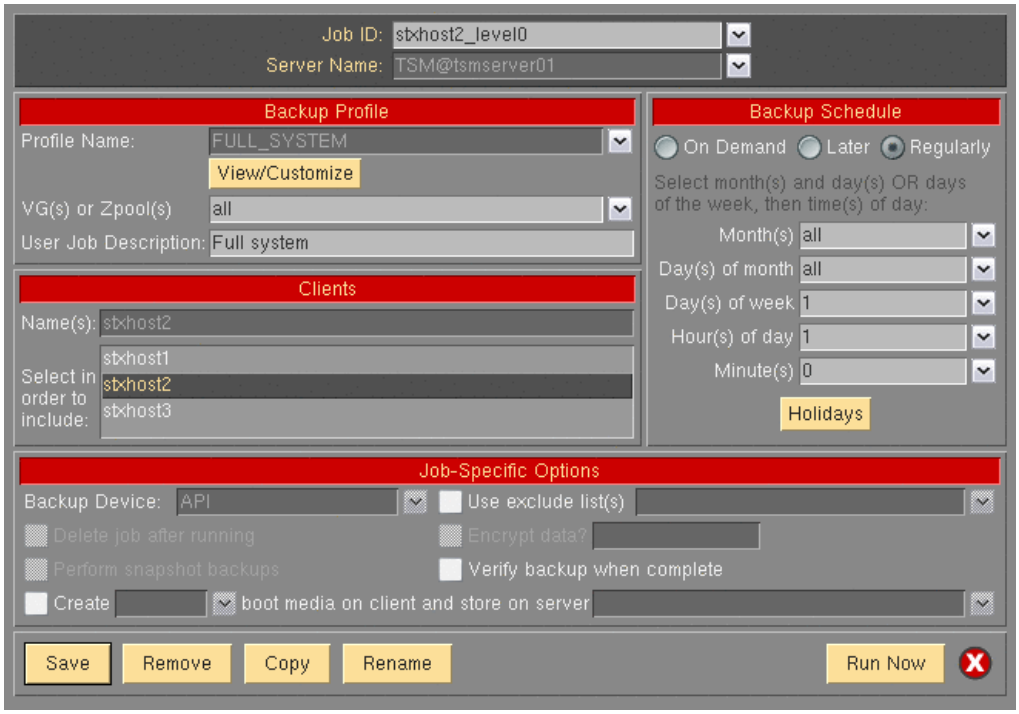
Before configuring a backup job, you must first have configured at least one TSM Client to backup and a TSM Server to backup to (even if the client and server are the same). There must also be at least one System backup profile (a default profile comes installed with the software). On the job configuration screen, you can customize the selected backup profile to apply changes which apply only to the job, if desired.

Creating a Backup Job

To create a backup job, either

1. Select Configure→Backup Jobs from the menu bar, or
2. Press the **Add** button on the Main Screen when the Job Information is displayed.

The following **Configure Backup Job** will be displayed:



To create a new backup job, enter the **Backup Job ID** in the entry field at the top. The Job ID is used as unique identifier for this job, and may consist of any letters or numbers except for a colon (:) or space (spaces will be automatically replaced with an underscore).

Next, you must select an entry in the **Server Name** field (see below). Additional required fields include the **Profile Name** and the **Clients** to backup. All other settings will provide a default value. If you did not define the **VG(s) or Zpools(s) to include** (or all) in the backup profile, you may need to enter this information now.

More details on the various entries which follow are described below. Remember, you may use QuickHelp anywhere on this screen for specific instructions or information on a specific option.

When all selections are complete, press the **Save** button at the bottom of the screen to save the profile and clear the current selections.

Selecting the Server or Device

Using the arrow button to the right of the **Server Name** field, you will get a pop-up list of all TSM servers and one addition entry "***local (client tape)***". When selecting "***local (client tape)"*** you may only select a single *Client*, and the *Backup Device* will be **SBTAPE**. Refer to Creating a Local System Backup below for more information.

If you select a *TSM Server*, you may select one or more clients to backup as part of the backup job, and the **Device Name** field will be disabled.

Selecting/Customizing the Backup Profile

You must assign a backup profile to the job. The profile will determine the specific backup options which apply to the backup type. Refer to the Volume Groups to Include in the Backup Profiles section for additional information. After selecting a profile, the **Volume Groups to Backup** and **User Backup Description** fields will be filled in automatically from the profile information (if provided there). You may override the profile data by simply changing the information in those fields. This will not change the information in the original profile.

If you want to change any of the default backup settings from the profile, you may select the **View/Customize** button. This will display the profile options screen and allow you to make any changes that will apply only to this job. You may use this option, for instance, to turn on SBAdmin backup compression (thereby overriding the TSM compression) even though other jobs that use the same profile will be unaffected. You can also use this option, to change only the **Incremental Backup Level** so that all incremental backups, even those at different levels, can use a single backup profile.

Selecting Clients to Backup

If you selected a TSM Server to backup to, you must make one or more selections from the ***Clients*** listbox. If you selected to backup to local tape, you may select only one client from the list. The selections will be displayed in the **Name(s)** entry field to indicate the order in which the client backups will be performed. If you want to change the order of the backups, just de-select and re-select the clients in the listbox until they appear in the desired order.

If you selected "**local (disk/tape)**" in the **Server** field, then you may only select one client from the list, since that client will be sending the backup to its own local tape drive.

Additional Options

Answers to the following question buttons may be used to override the default actions taken during a backup:

- ***Delete job after running***: This option is only available when a backup job has been configured to run "*Later*", or once-only. If so, check this option to have the job configuration removed from the system upon completion of the backup job. This is useful if you are creating temporary backup jobs that are never to be used again.

- ***Perform snapshot backups***: This option is only available if snapshot backups have been configured for one or more of the selected clients. By default, all backups are performed using the active (online) copy of a filesystem or logical volume (even when snapshot backups have been configured). To create snapshots of each logical volume before backing it up, check this button.